Azure Networking

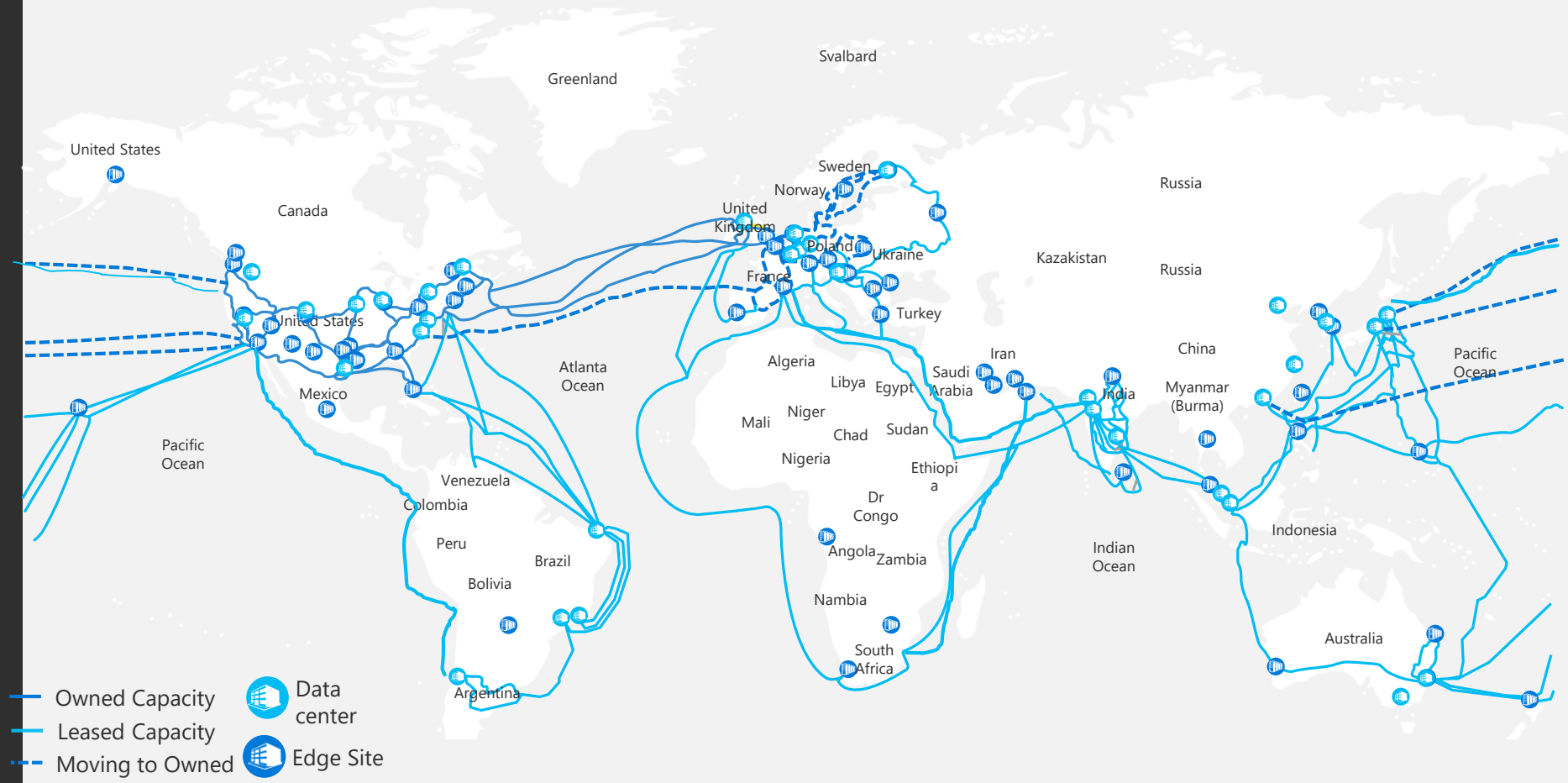
Joe Losinski
Partner Technology Strategist

Microsoft Global Network

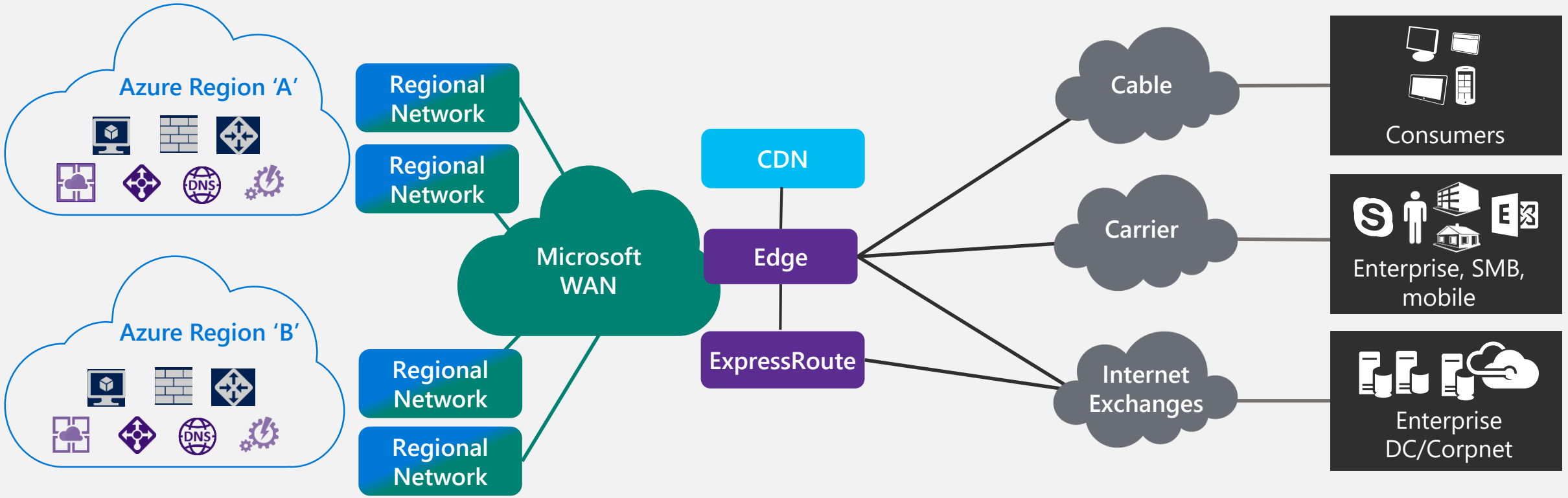
One of the largest private networks in the world

- 8,000+ ISP sessions
- 130+ edge sites
- 44 ExpressRoute locations
- 33,000 miles of lit fiber
- SDN Managed (SWAN, OLS)

DCs and Network sites not exhaustive



Azure Networking



DC Hardware	Services	Intra-Region	WAN Backbone	Edge and ExpressRoute	CDN	Last Mile
• SmartNIC/FPGA • SONiC	• Virtual Networks • Load Balancing • VPN Services • Firewall • DDoS Protection • DNS & Traffic Management	• DC Networks • Regional Networks • Optical Modules	• Software WAN • Subsea Cables • Terrestrial Fiber • National Clouds	• Internet Peering • ExpressRoute	• Acceleration for applications and content	• E2E monitoring (Network Watcher, Network Performance Monitoring)

Regional Networks

High Availability Design

Regional network gateway

Massively parallel, hyper scale DC interconnect (up to 1.6 Pb/s)

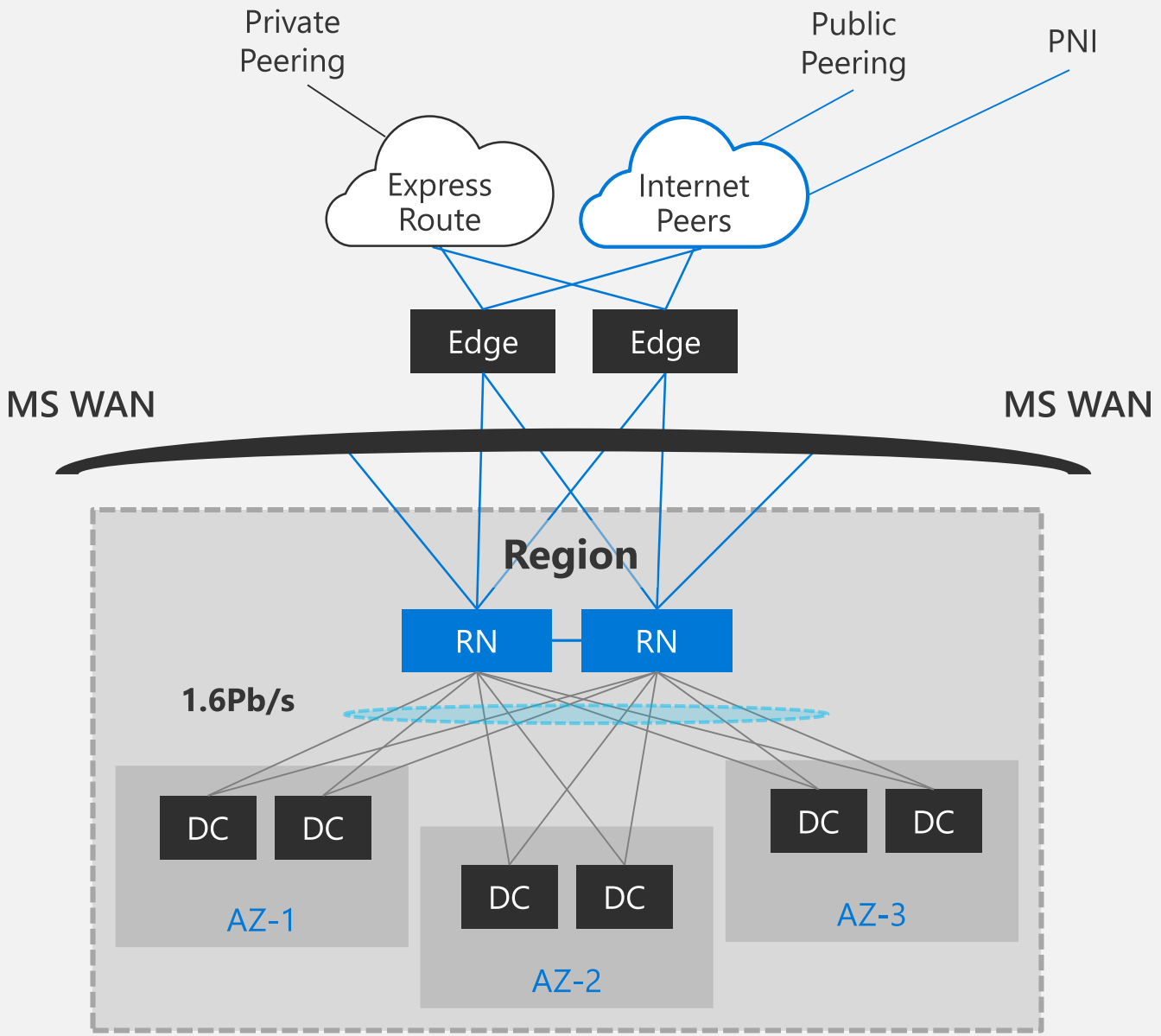
Space and power protected

RNG data centers

T-shirt sized (S,M, L, XL)

Contains server racks, DC NW

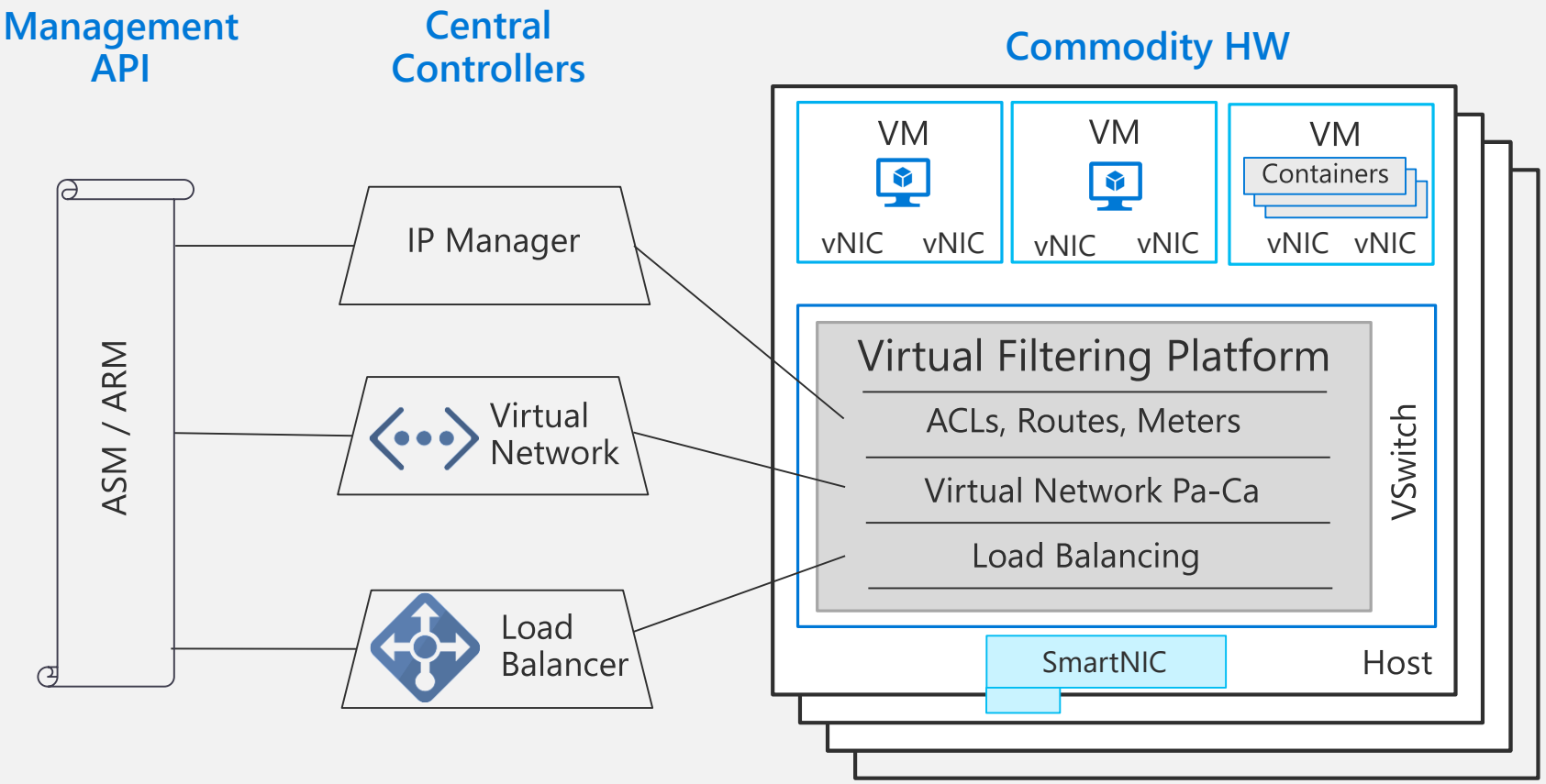
RNGs are sized to support growing the region by adding data centers



Software Defined Networking (SDN)

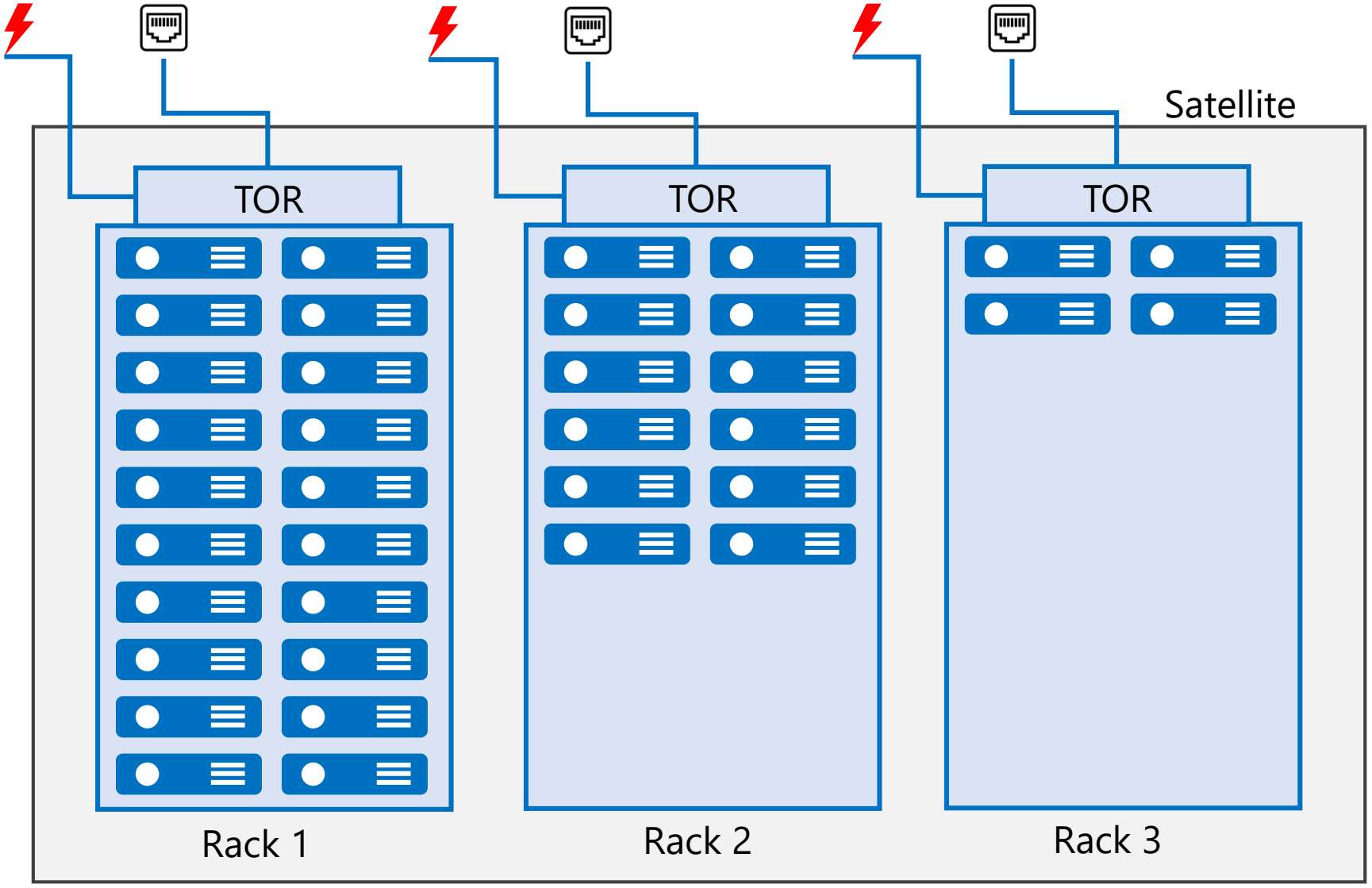
Azure SDN
Basis of all NW virtualization in our datacenters

Decoupled
SDN allows compute to evolve and converge to a single allocator



Key to flexibility and scale is Host SDN

Satellite - Physical layout

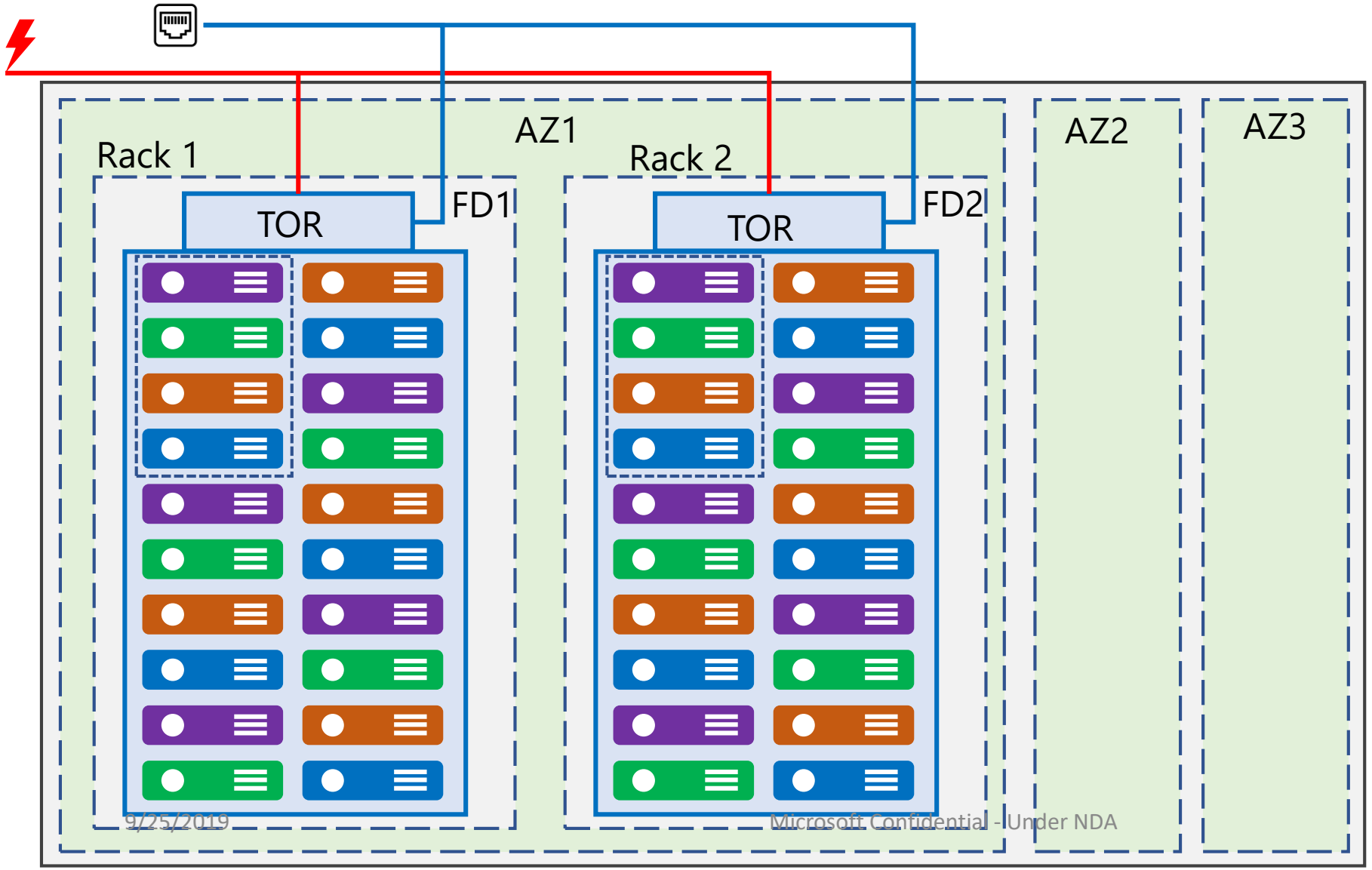


A **satellite** physically consists of multiple **racks**, ideally physically connected to separate network & power/cooling

Number of **servers** in the rack based on capacity needed and SKU

Satellite(s), rack(s), server(s), ToR(s) will be modelled as explicit Azure Resources

Satellite - Logical View

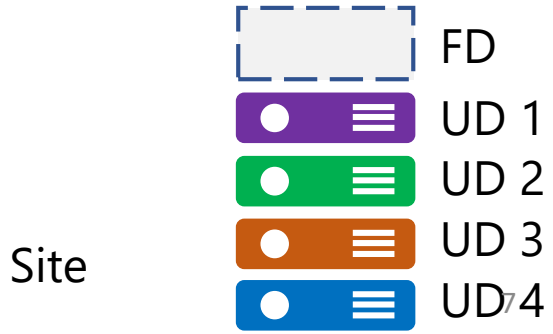


A **satellite** is logically divided into multiple AZs (same as the homed Azure region)

AZs contain racks

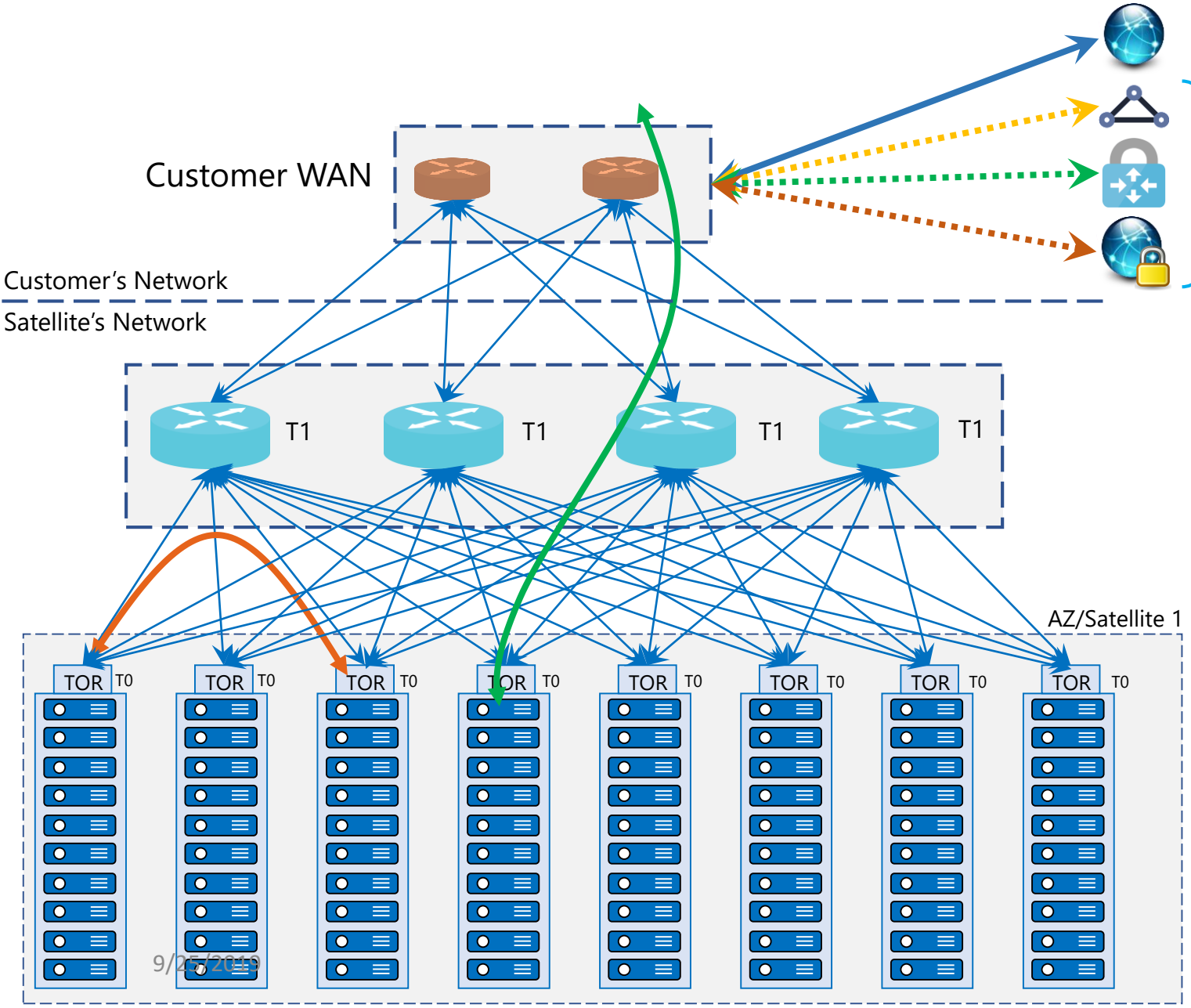
Each rack is a single **fault domain (FD)**

Rack has servers across multiple **update domains (UD)**



Site

Satellite – Intra-satellite connectivity



Multi-stage switching network to provide scalability and redundancy

Each fault domain is connected to T1 routers.

All T1 routers roll into 2 T2 routers, which are connected to Customer's WAN network.

Customer's WAN network provides Satellite connectivity to Internet and to Azure DC.

Robust networking infrastructure services

Virtual Network

Provision private networks, optionally connect to on premise datacenters. NSG, User Defined Routes, & IP addresses.

Load Balancer

Deliver high availability and network performance to your applications

Application Gateway/WAF

Build scalable and highly-available web front ends in Azure

DDoS Protection

Protect your Azure resources from DDoS attacks

VPN Gateway

Establish secure, cross-premise connectivity

Azure DNS

Host your DNS domain in Azure

Content Delivery Network

Ensure secure, reliable content delivery with broad global reach

Traffic Manager

Route incoming traffic for high performance and availability

ExpressRoute

Dedicated private network fiber connections to Azure

Network Watcher

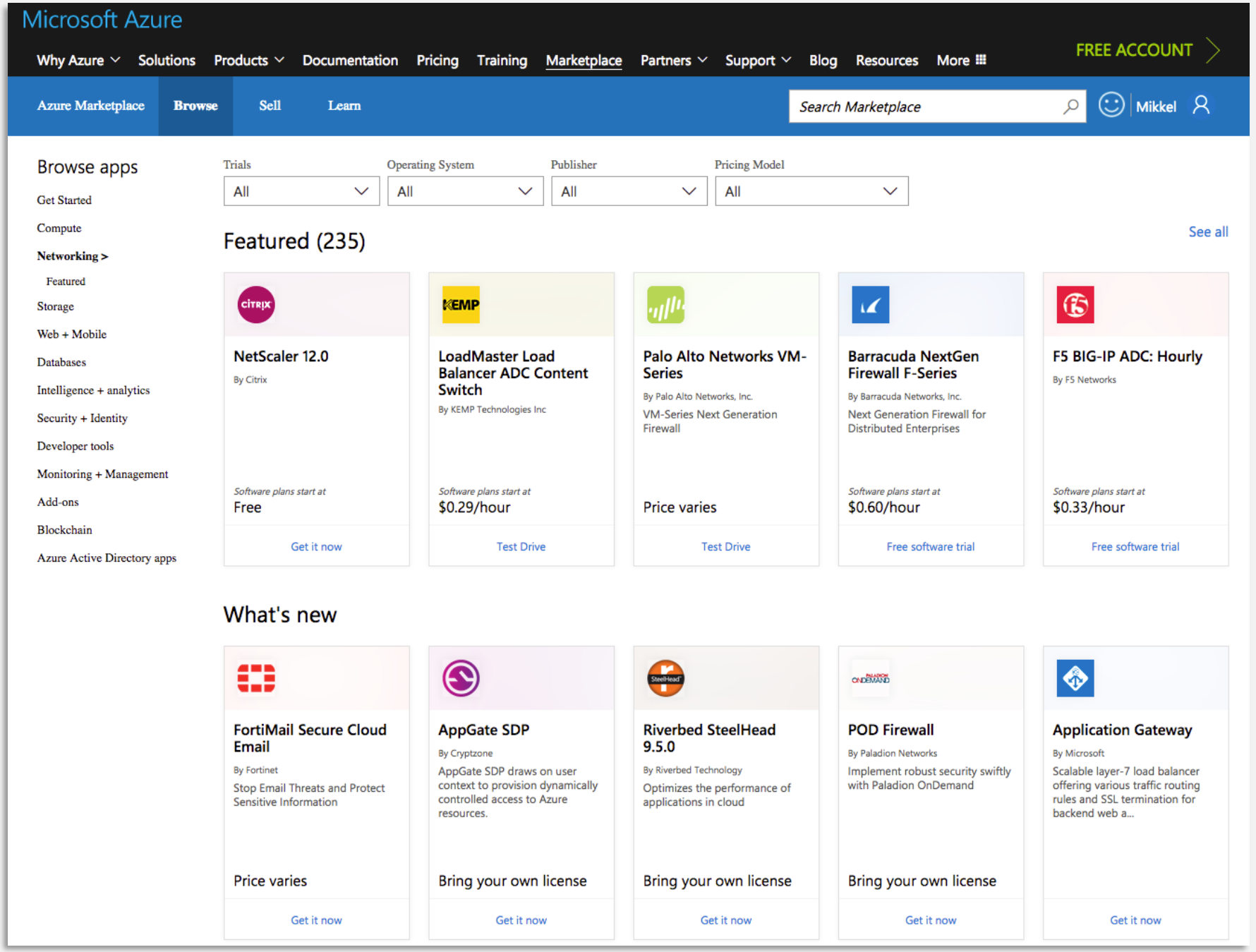
Network performance monitoring and diagnostics solution

Network Virtual Appliances

Best-of-breed partner appliances through the Azure Marketplace

Extend on premises to Azure using a familiar feel

Easy to deploy, configure and manage

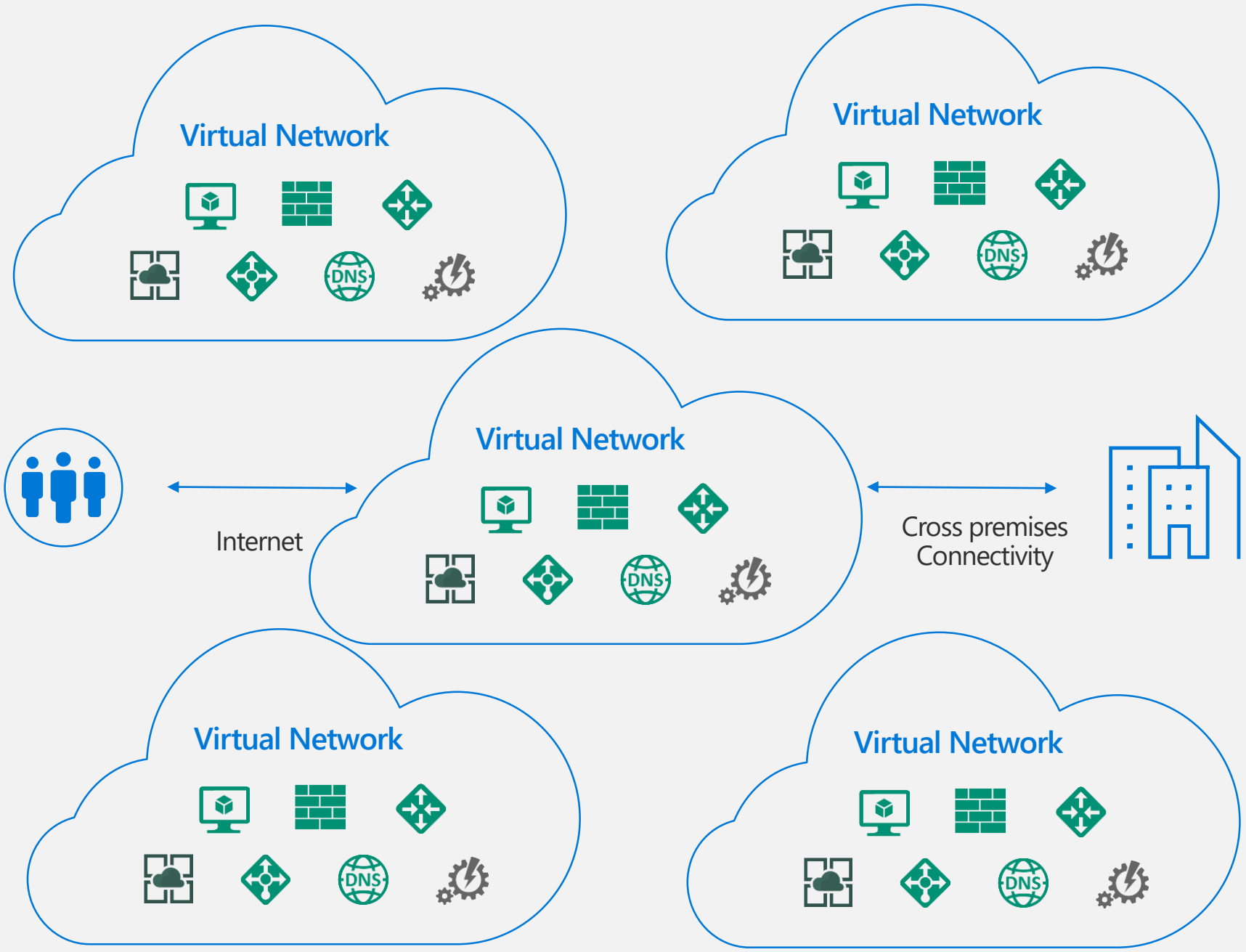


Your Network in Azure

Secure per customer virtual datacenter in the cloud

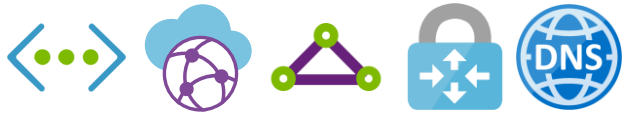
Instantiate and configure complex topologies in minutes

Rich security and networking services

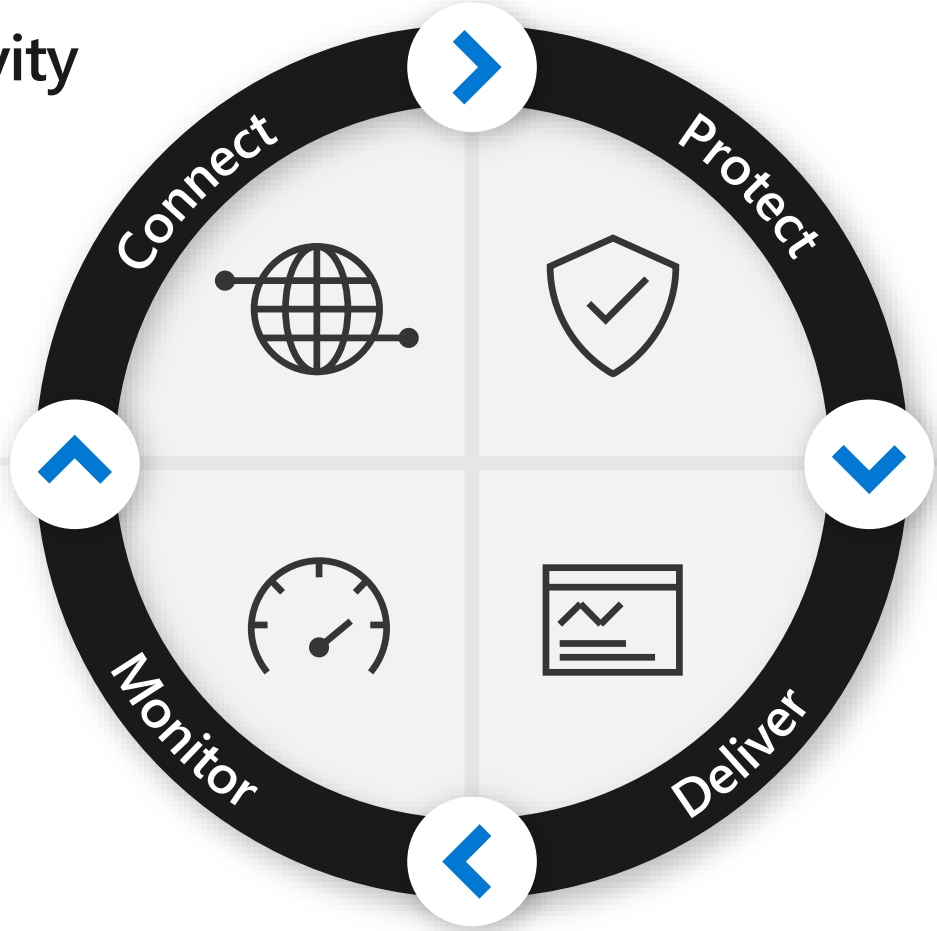


Azure Networking Services

Distributed cloud connectivity



VNET | Virtual WAN | Express Route | VPN | DNS



Control and protect your cloud resources

DDoS | Firewall | NSG | WAF | VNET Endpoints

Measure – Monitor – Troubleshoot – Act

Azure Monitor | Network Monitor | Virtual Network TAP

Fast, secure and easy scaling of any web app

Load Balancer | Application Gateway | Traffic Manager | CDN | Front Door Service

OSI Model

Please

Do

Not

Touch

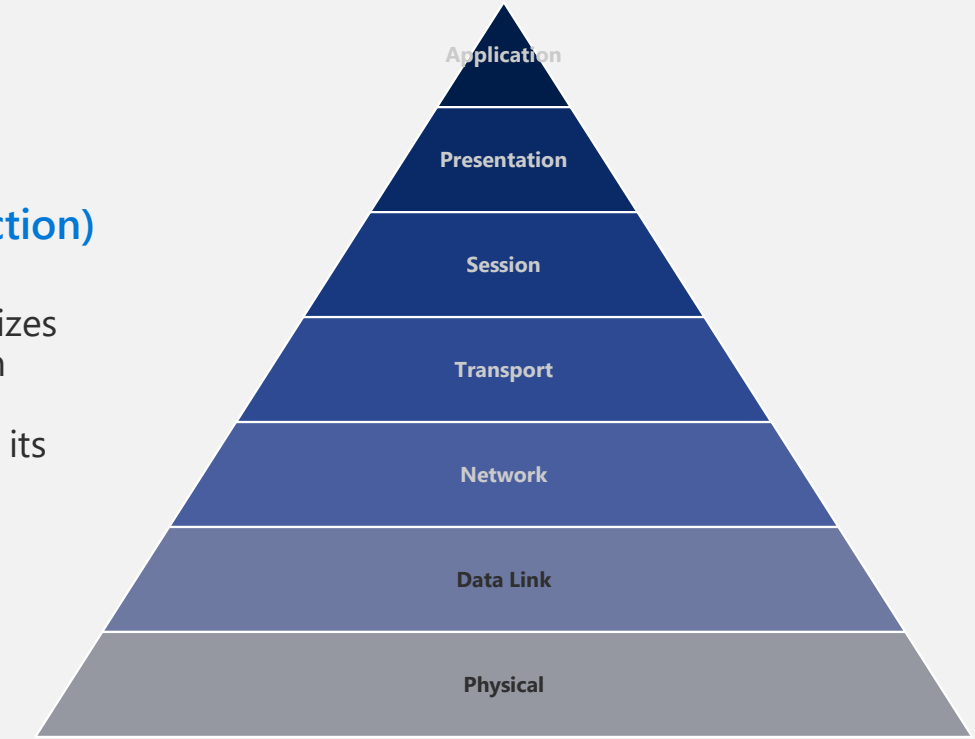
Steve's

Pet

Alligator

OSI (Open Systems Interconnection)

is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.



Layer	TCP/IP Model	OSI Model	Network Comm.	Protocols and Services
7	Application Layer	Application	Data	HTTP, FTP, Telnet, NTP, DHCP, PING
6		Presentation	Data	
5		Session	Data	
4	Transport	Transport	Segment/Datagram	TCP, UDP
3	Internet	Network	Packets	IP, ARP, ICMP, IGMP
2	Network Access (Link)	Data Link	Frames	Ethernet
1		Physical	Symbol/Bits	

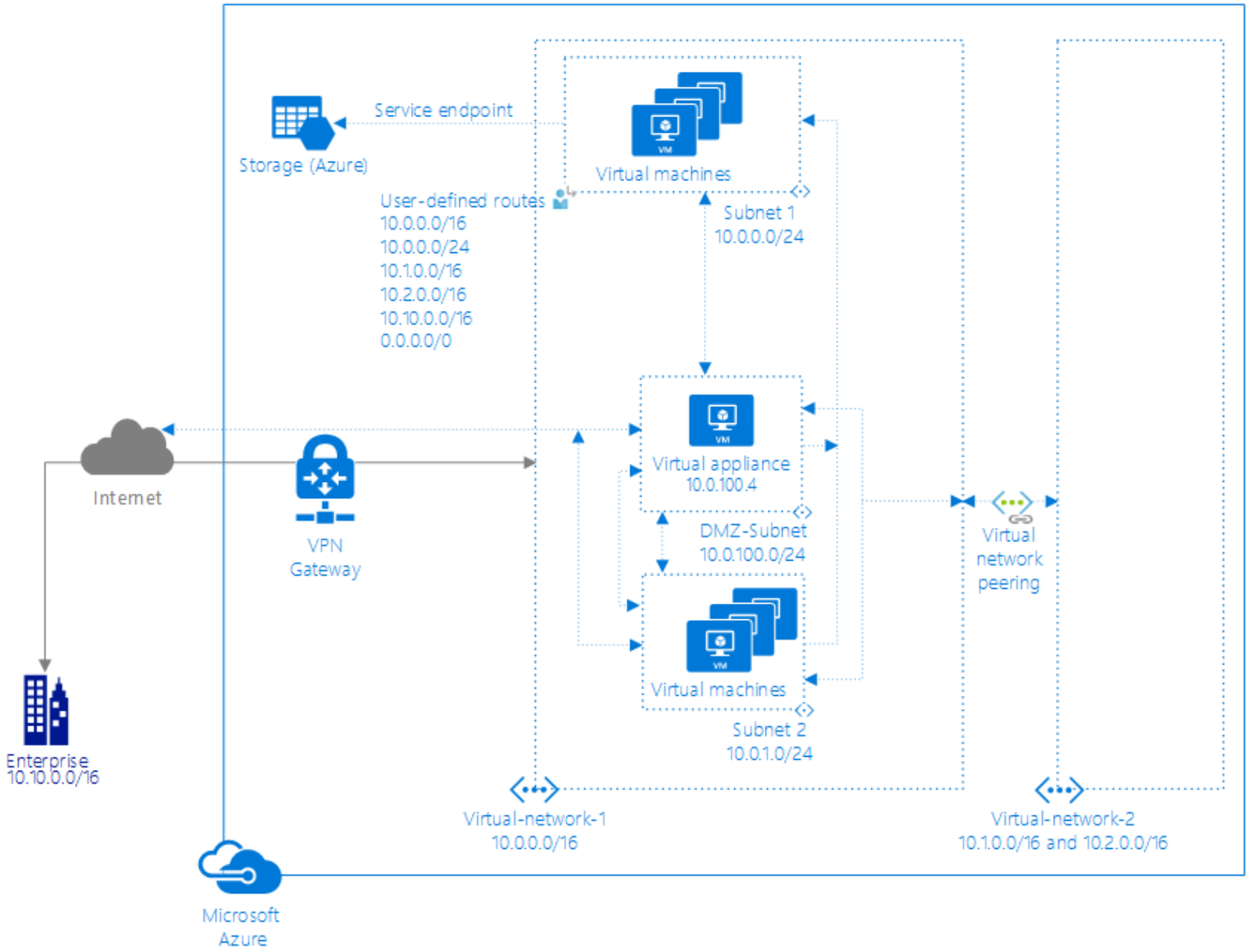
Azure Network Framework

VNET

Subnet

IP Address

Public vs Private IPs

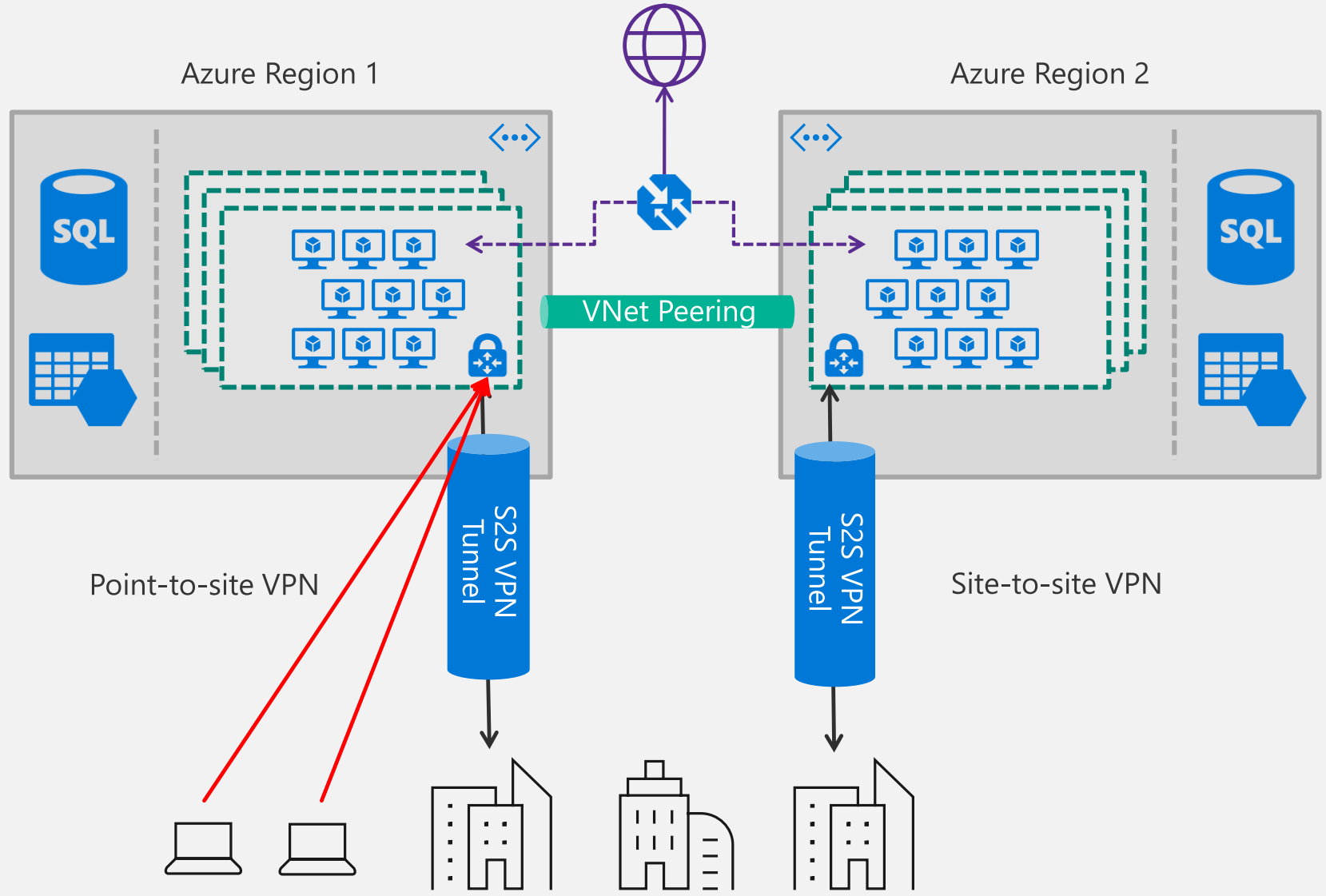


Connectivity

From on-premises

Within Azure

VPN and Point-to-site (P2S)

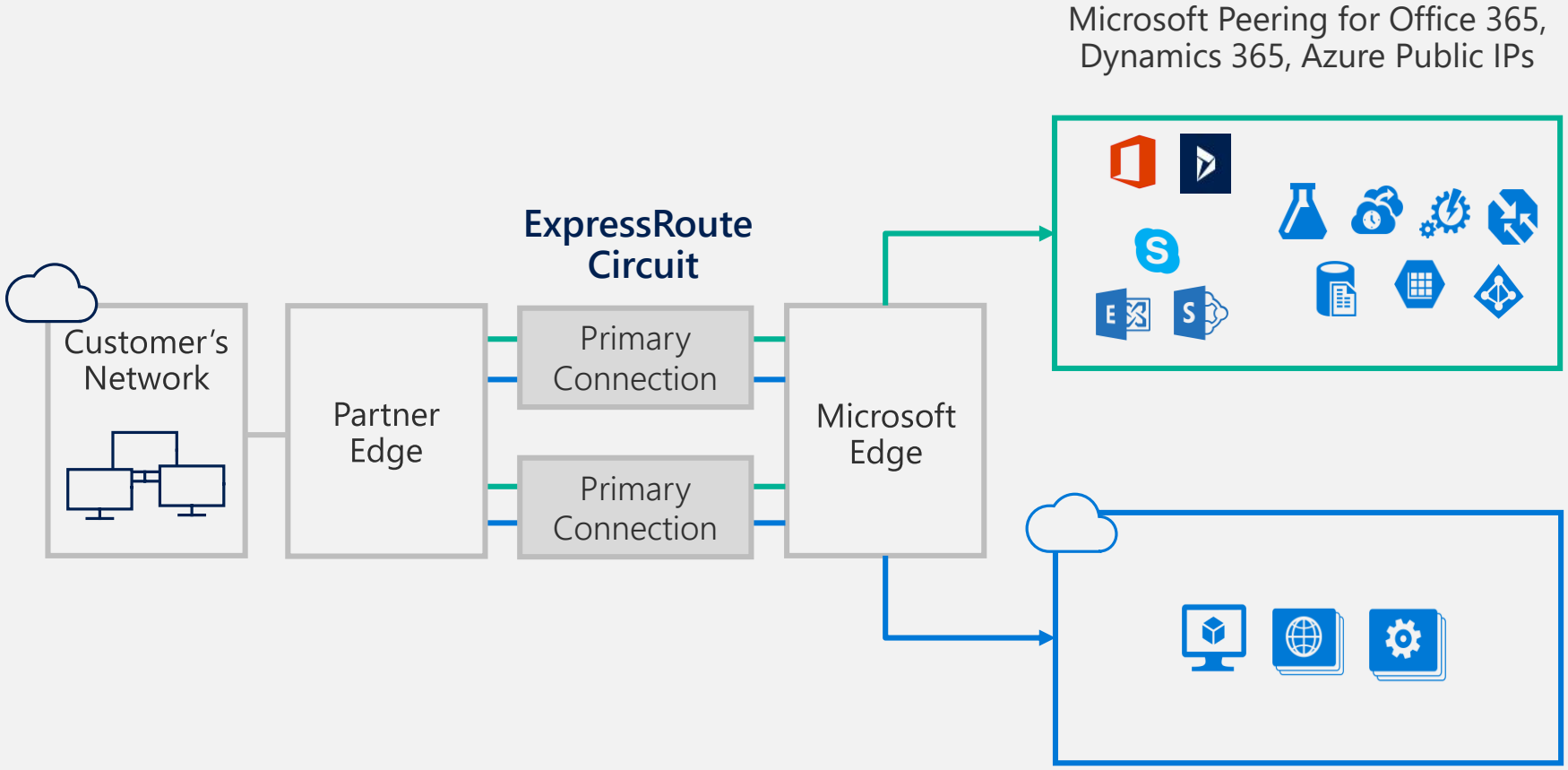


Connectivity

From on-premises

Within Azure

ExpressRoute



Private connectivity to Microsoft bypassing the Internet

Predictable performance

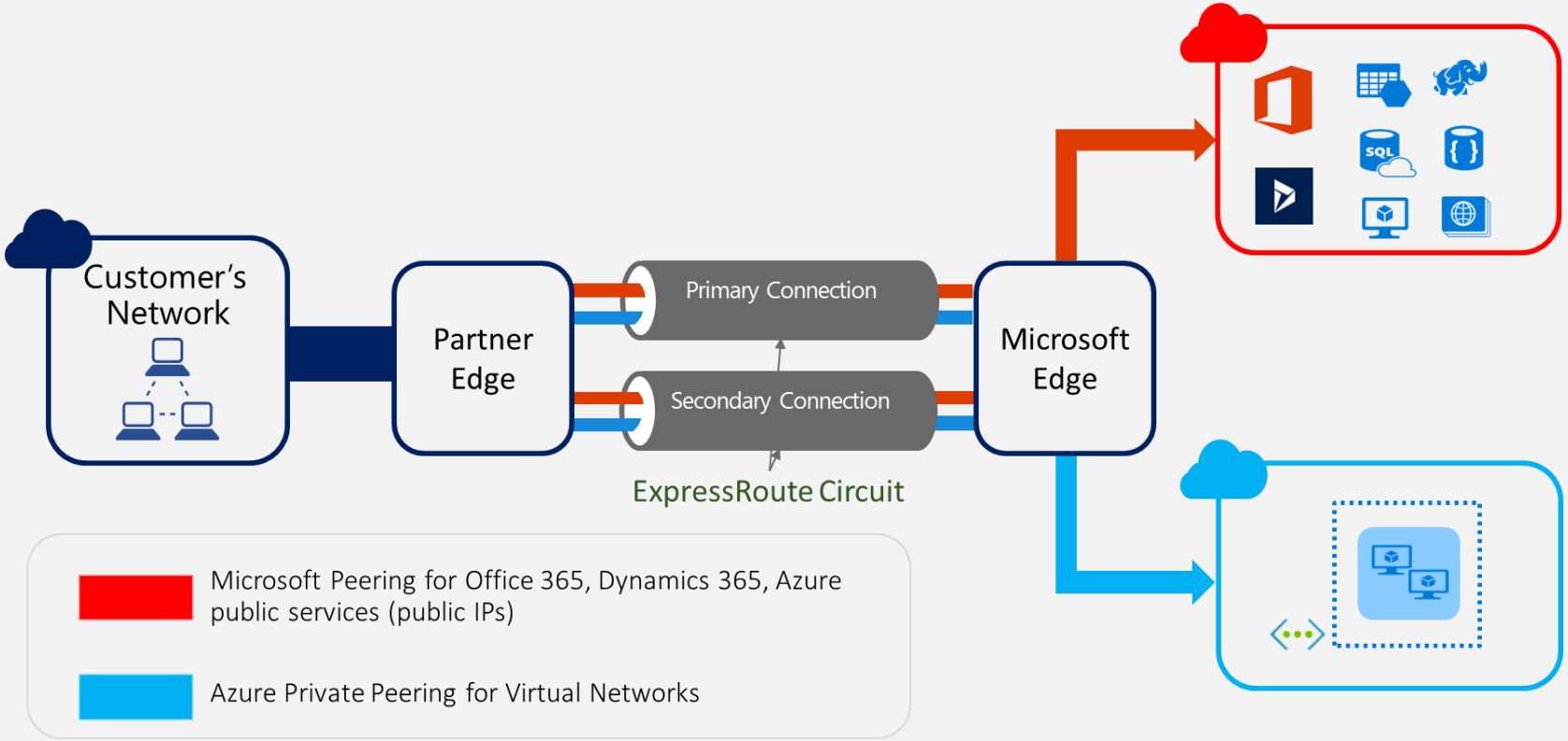
Enterprise-grade resiliency with SLA

Large and growing ExpressRoute partner ecosystem

Azure Network Framework

UDRs - User Defined Routes

VPN/ExpressRoute

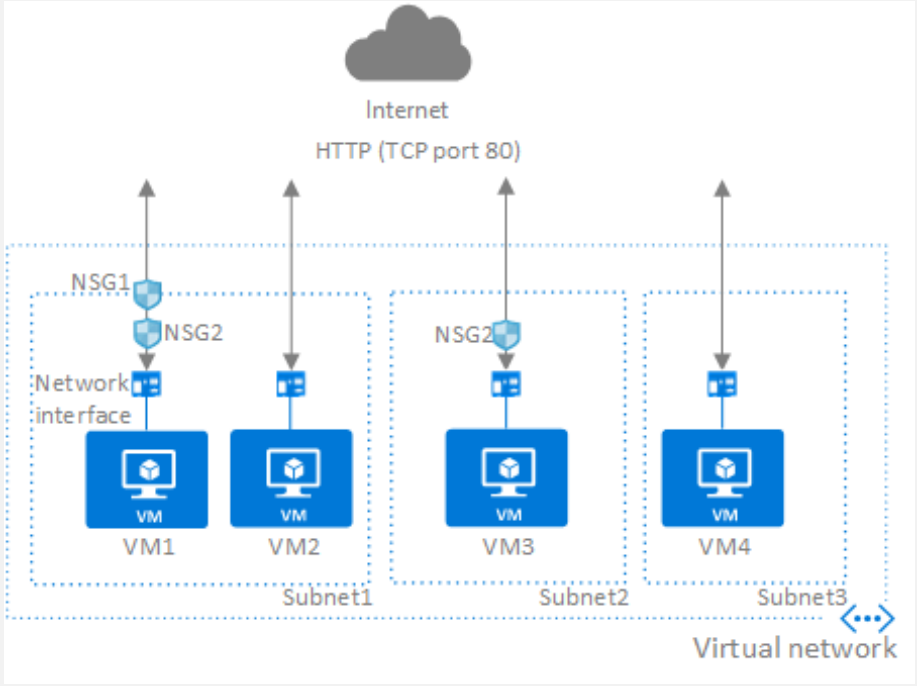


Azure Network Framework

NSG (Network Security Groups)

Service Tags

Application Security Groups

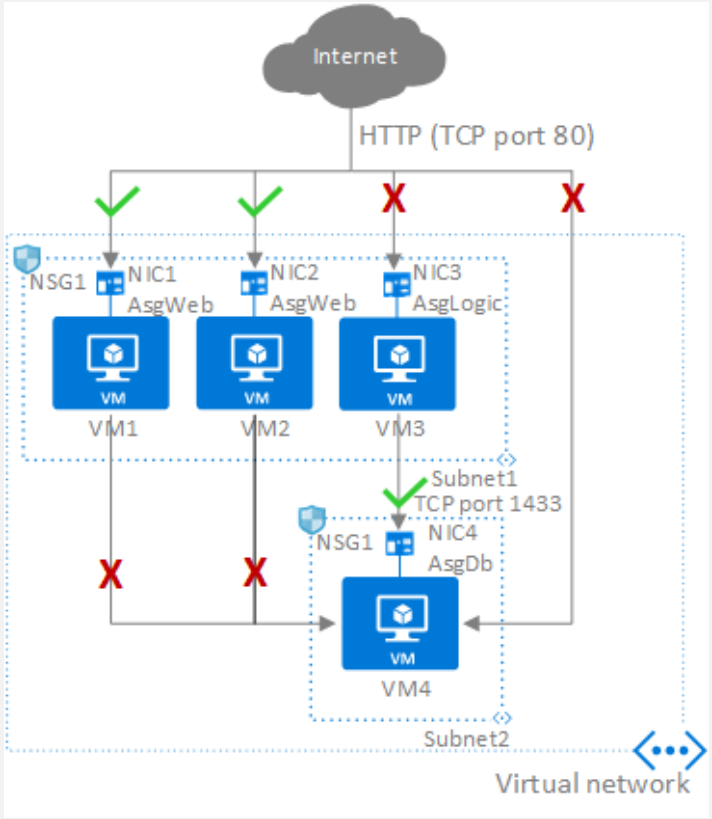


NSGs

- Prioritized Inbound/Outbound Rules
- Assigned to NIC or Subnet
- Default Security Rules

NSG Options

- Augmented Security Rules
- Service Tags
- Application Security Groups



Connectivity

From on-premises

Within Azure

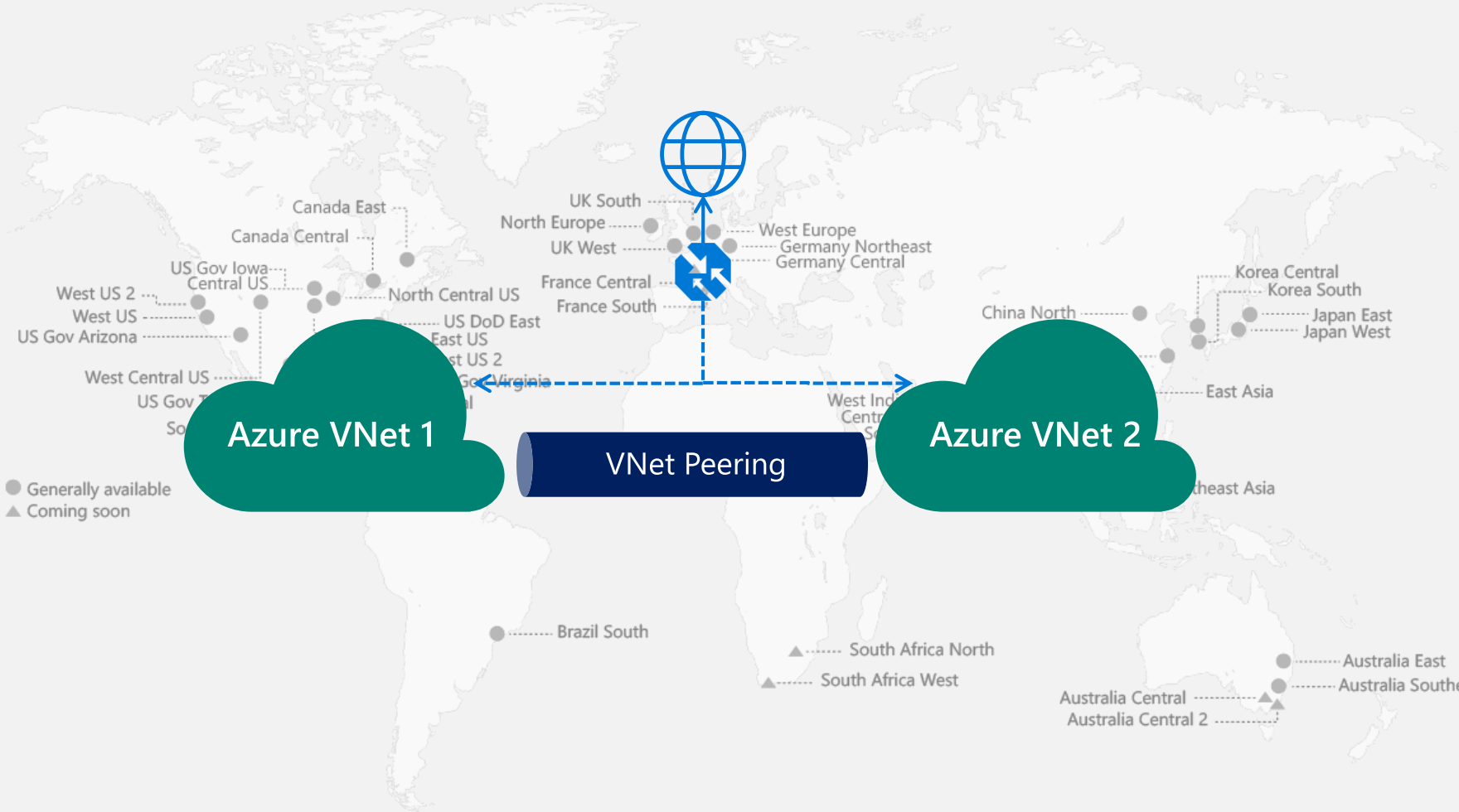
ExpressRoute | 200+ Partners

Connectivity

From on-premises

Within Azure

Global VNet Peering



VNets in different regions can now be peered directly

Simple and quick to configure

Routed through the Azure backbone

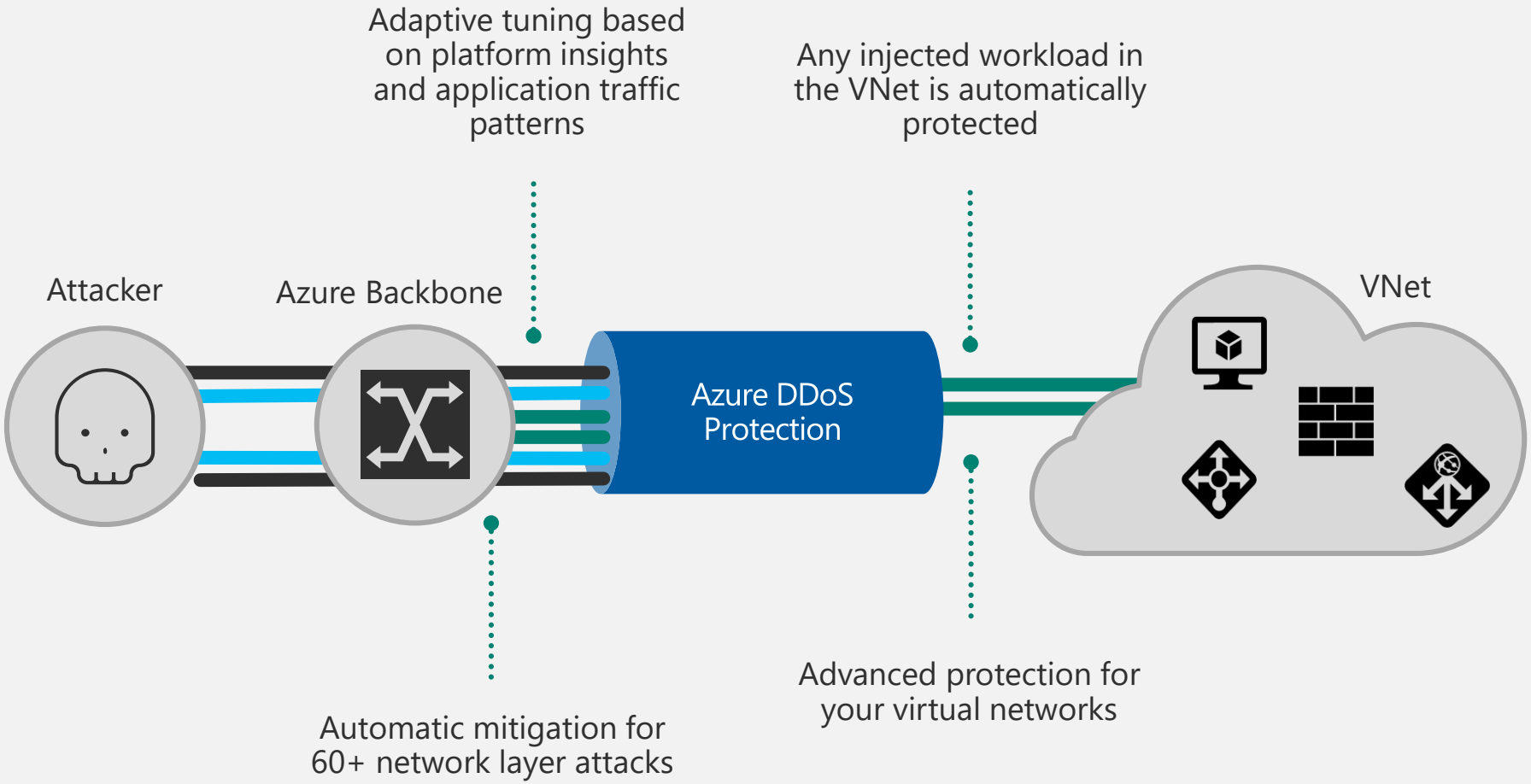
Protecting your application

From the Internet

Within the VNet

Within Azure

DDOS Protection



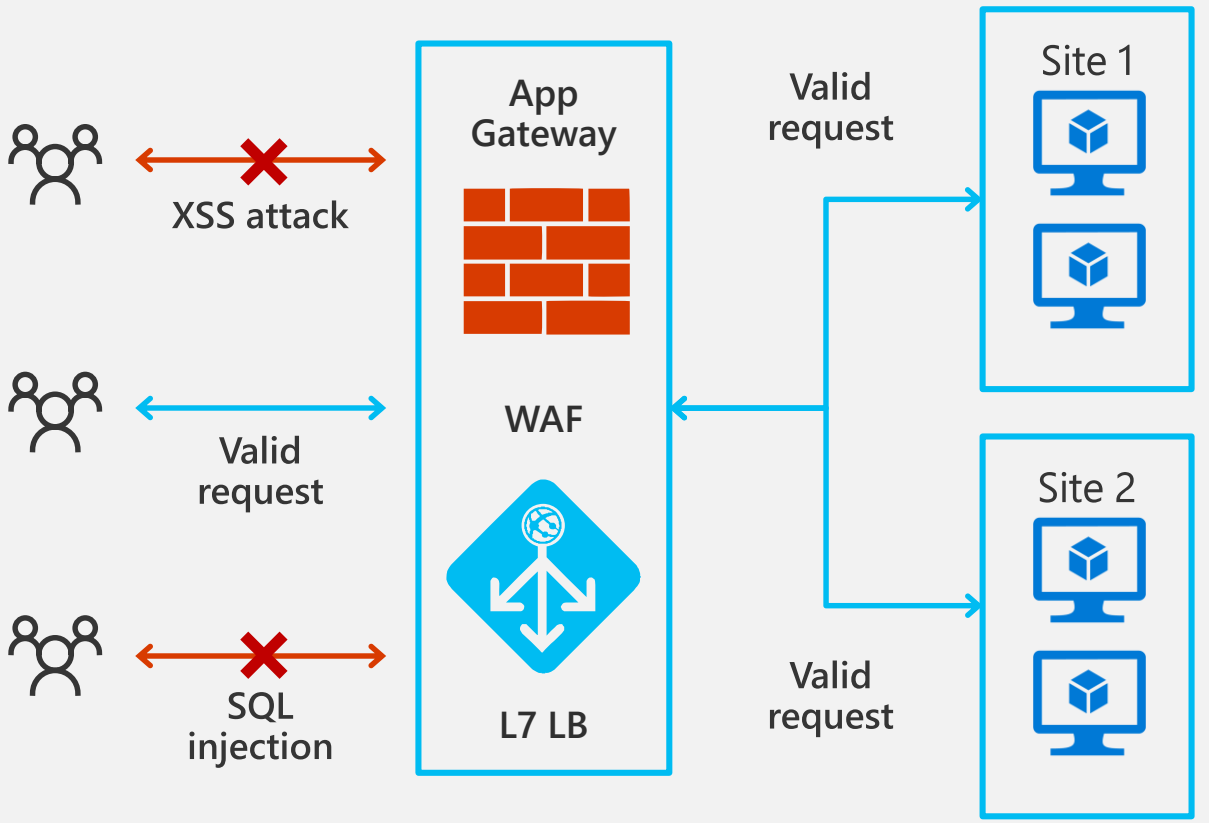
Protecting your application

From the Internet

Within the VNet

Within Azure

Web Application Firewall



Protect your app against prevalent X- Site Scripting and SQL Injection attacks

Blocks threats based on Top 10 OWASP signatures

Integrated with Azure Security Center

Real-time logging with Azure Monitor

Platform managed, scalable and highly available

Protecting your application

From the Internet

Within the VNet

Within Azure

Simplified Security Group Management

Network Security Groups (NSG)

IP based network ACL

Attach: Subnet and NICs

Service Tags

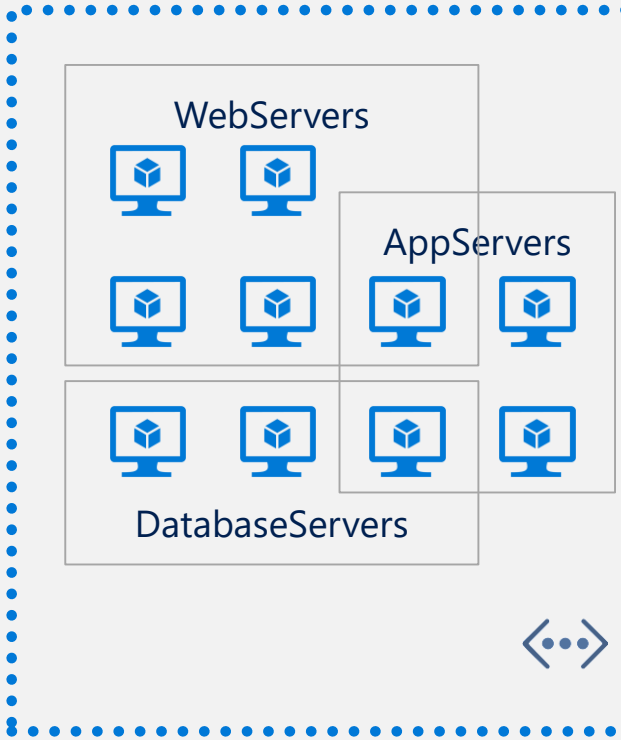
Named monikers for Azure service IPs

SQL, Storage, Traffic Manager supported

Application Security Groups (ASG)

Named monikers for custom grouping of VMs

Natural expression of application security



	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

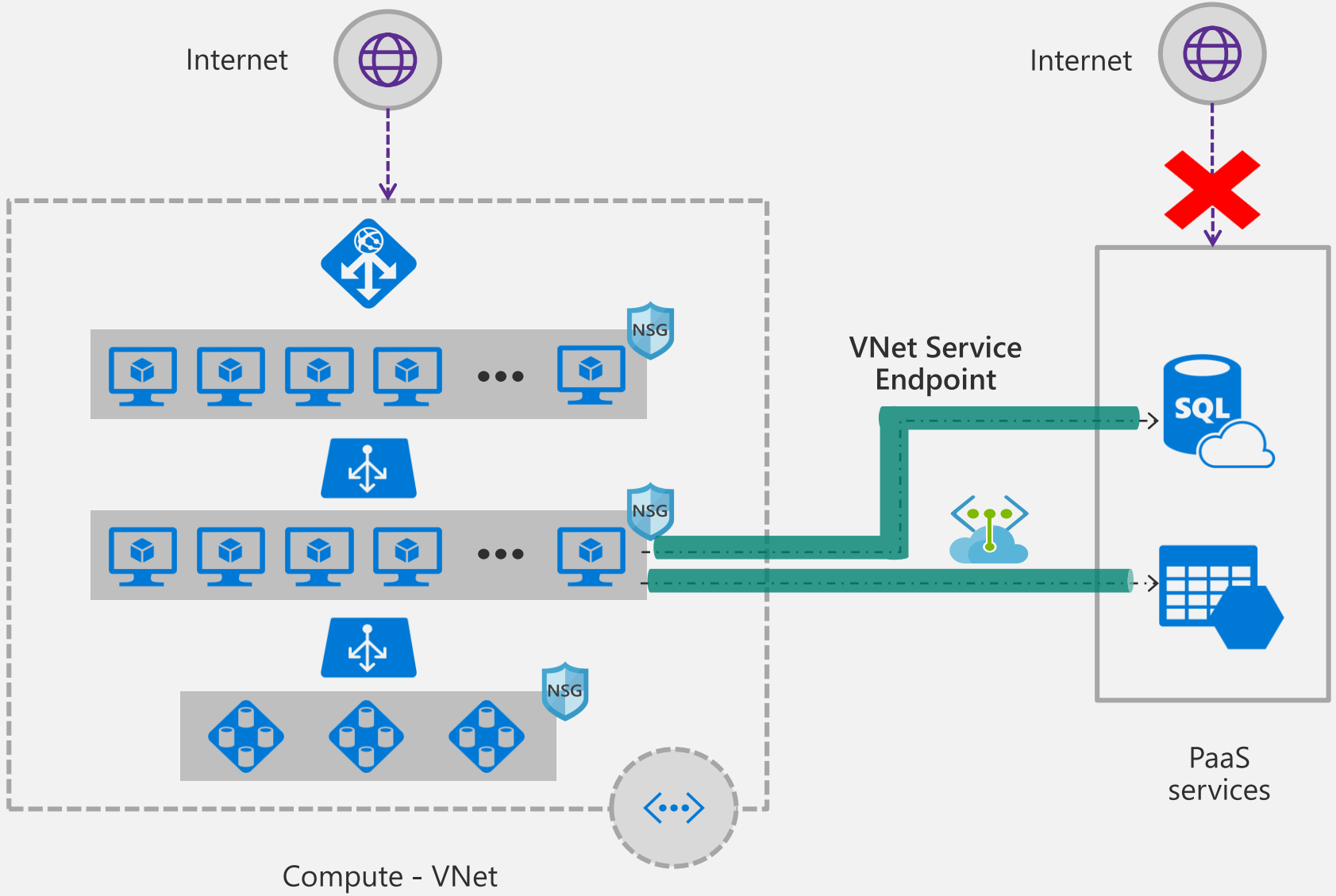
Protecting your application

From the Internet

Within the VNet

Within Azure

Securing PaaS Services



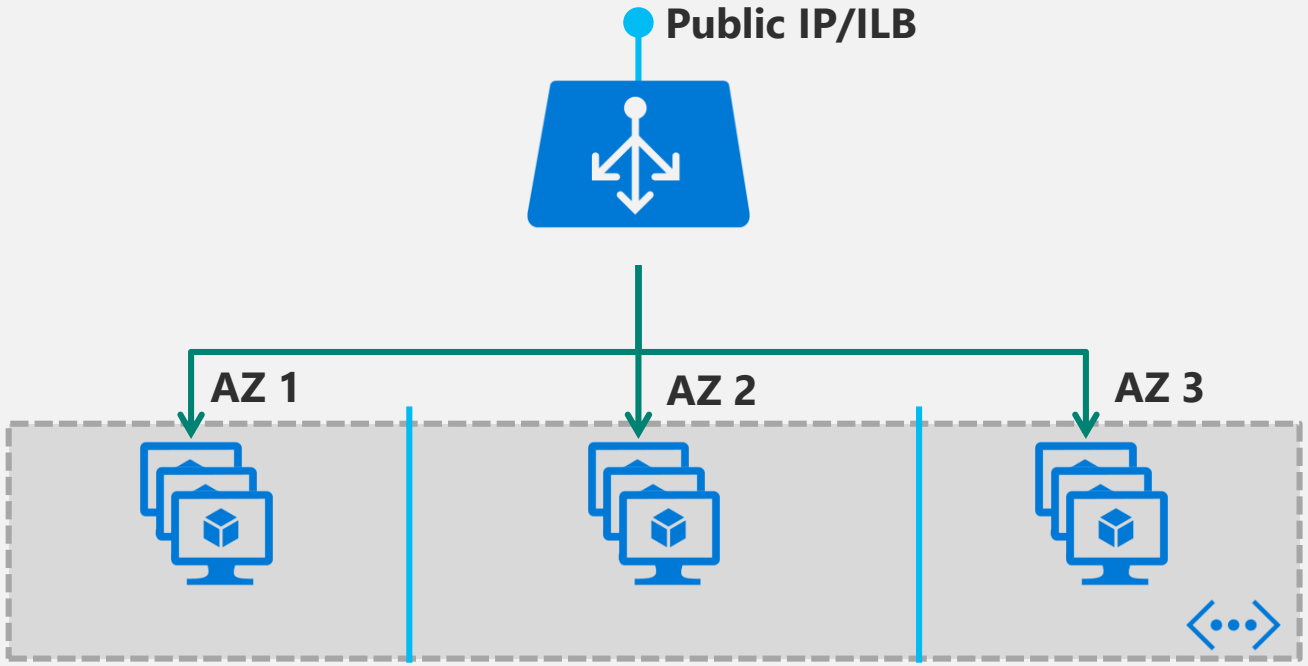
Availability

Application

Network

Zones

Standard Load Balancer



10x scale improvements—Increase from 100 to 1000 backend VMs

High availability through regional *anycast* IPs — single IP across AZs

Drastically simplified NVA Resiliency — HA Ports

Extensive health and diagnostic metrics

Availability

Application

Network

Zones

Availability Zones with Traffic Manager & Load Balancer

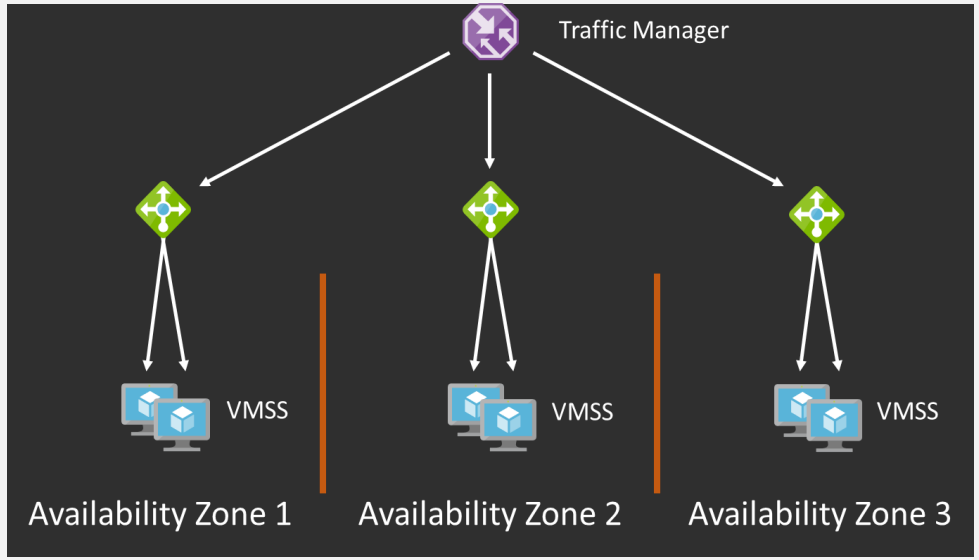
Traffic Manager

VMSS per Zone

TM profile for High Availability

Zonal VIP / VMSS

DNS name for cross-zone VMSS



Load Balancer - Standard

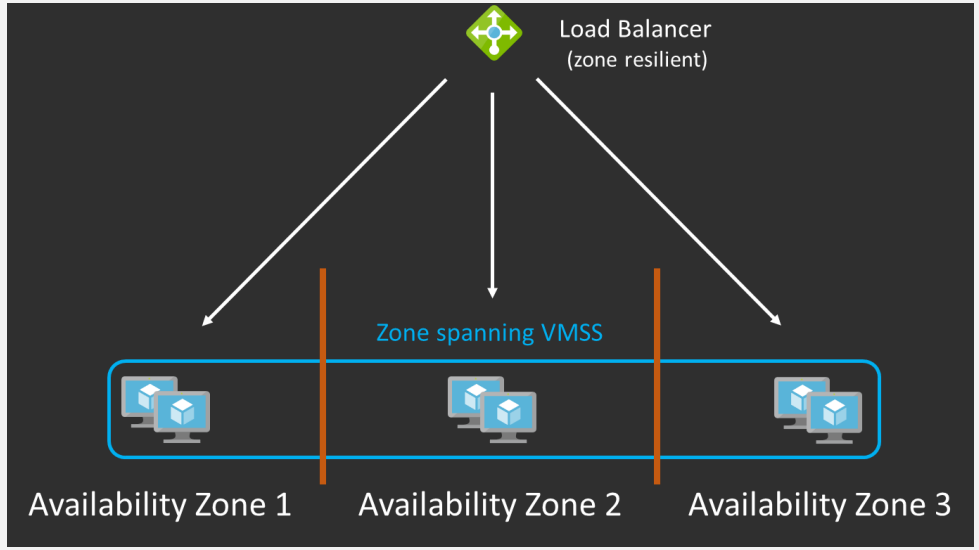
VMSS spans Zones

Load balancing across zones

Zone resilient VIPs

Single DNS name

VMSS limited to 1000 instances



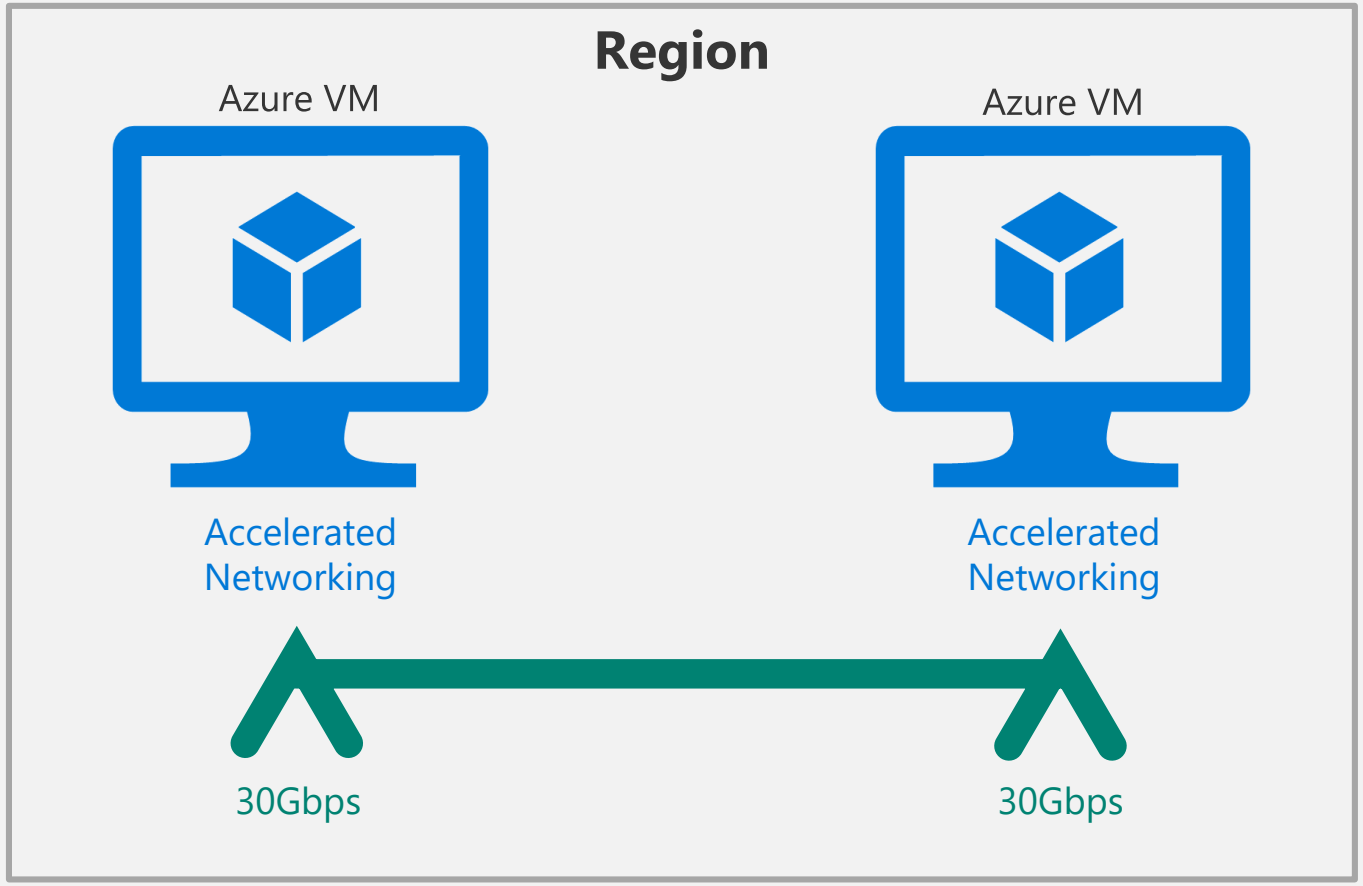
Performance and Monitoring

Performance

Monitoring

Accelerated Networking

30 Gbps VM to VM bandwidth!



Performance and Monitoring

Performance

Monitoring

Monitoring your resources with Azure Monitor

Public IP Address

06 AM

AVAILABILITY (AVG)	BYTE COUNT (SUM)	PACKET COUNT (SUM)	SYN COUNT (SUM)
WEBSITEIP	WEBSITEIP	WEBSITEIP	WEBSITEIP
99.99	157.06 G	19.27 M	105.59 k

Audit Logs

Available for all resources

Load Balancer

BYTE COUNT (COUNT)	DIP AVAILABILITY ...	PACKET COUNT (COU...	SNAT CONNECTION C...	SYN COUNT (COUNT)
WEBSITELOADBALANCER	WEBSITELOADBALANCER	WEBSITELOADBALANCER	WEBSITELOADBALANCER	WEBSITELOADBALANCER
102.95 k	25.78 k	102.95 k	257.56 k	102.95 k

Virtual network gateway

TUNNEL BANDWIDTH ...	TUNNEL EGRESS BYT...	TUNNEL EGRESS PAC...	TUNNEL EGRESS TS ...	TUNNEL INGRESS BY...	TUNNEL INGRESS PA...	TUNNEL INGRESS TS...
DEMOVNET1GW	DEMOVNET1GW	DEMOVNET1GW	DEMOVNET1GW	DEMOVNET1GW	DEMOVNET1GW	DEMOVNET1GW
2 B/s	98.3 KB	2.88 k	0	92.2 KB	2.96 k	0

Application Gateway

THROUGHPUT (AVG)
REGION-APPGW-0
260 B/s

Traffic Manager

ENDPOINT STATUS B...	QUERIES BY ENDPOI...
DMO2017IGNITE	DMO2017IGNITE
1	6

Network Interface Card

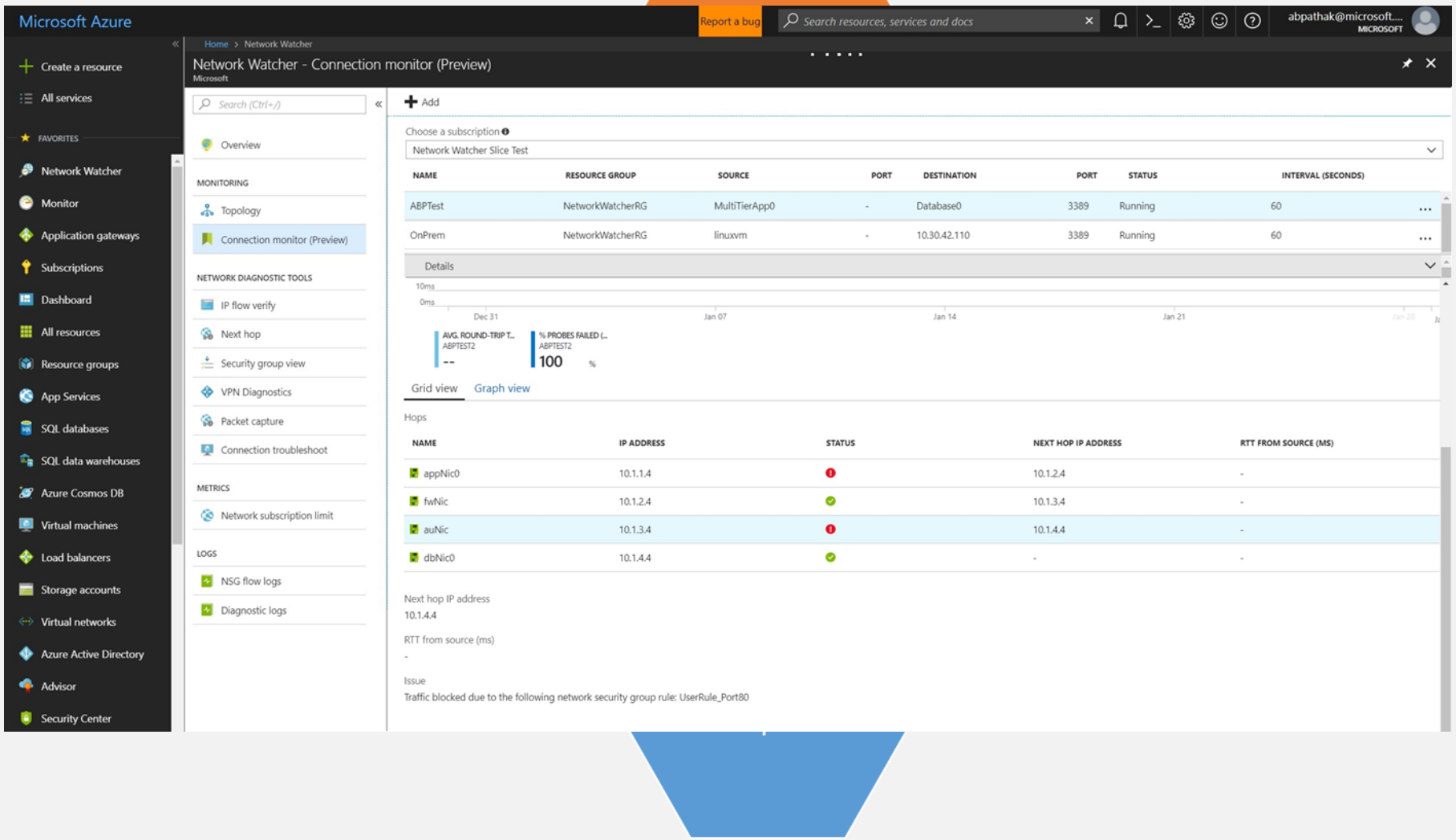
BYTES RECEIVED (S...	BYTES SENT (SUM)
WEBSITE859	WEBSITE859
428.65 M	18 G

Performance and Monitoring

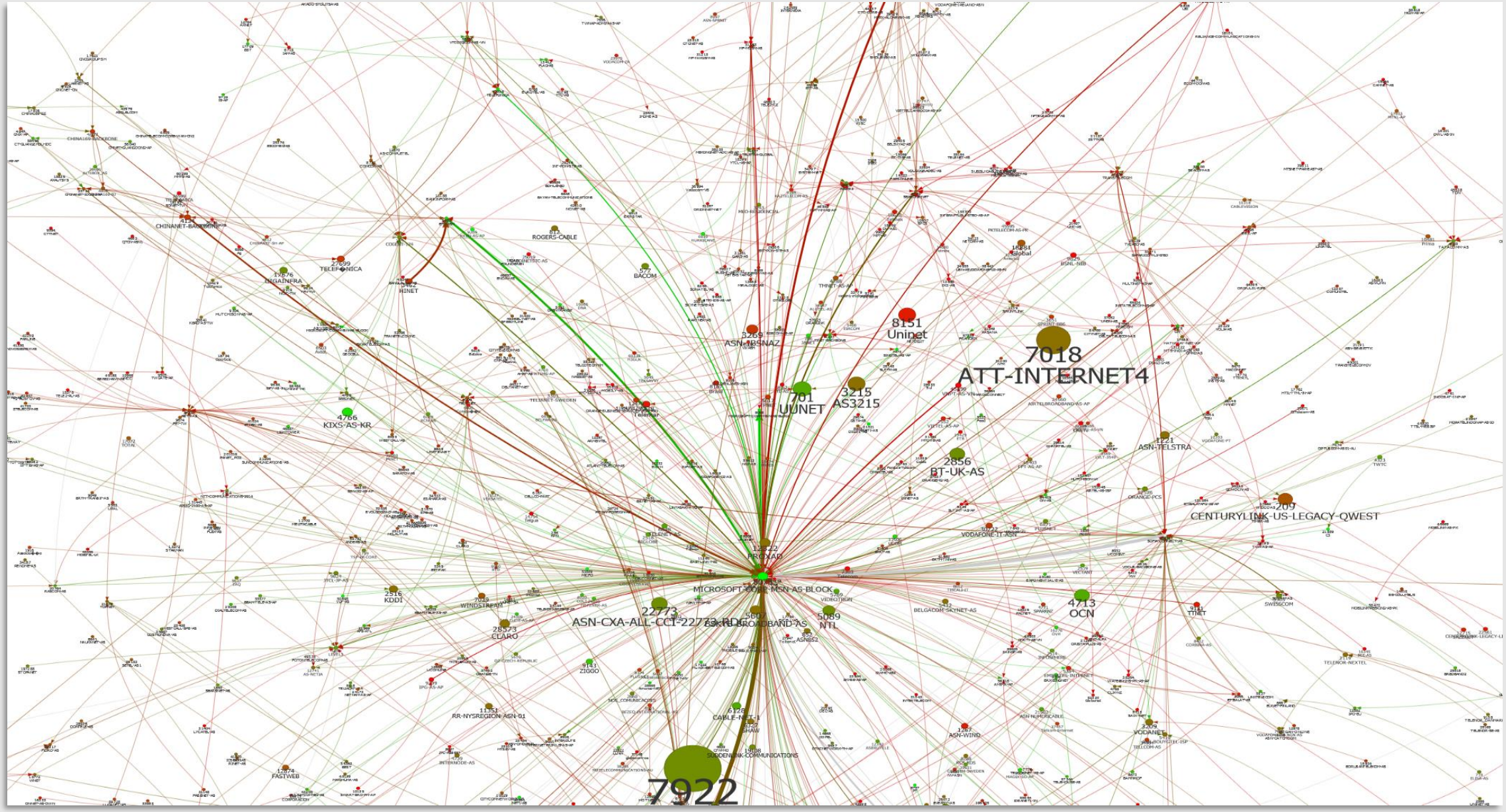
Performance

Monitoring

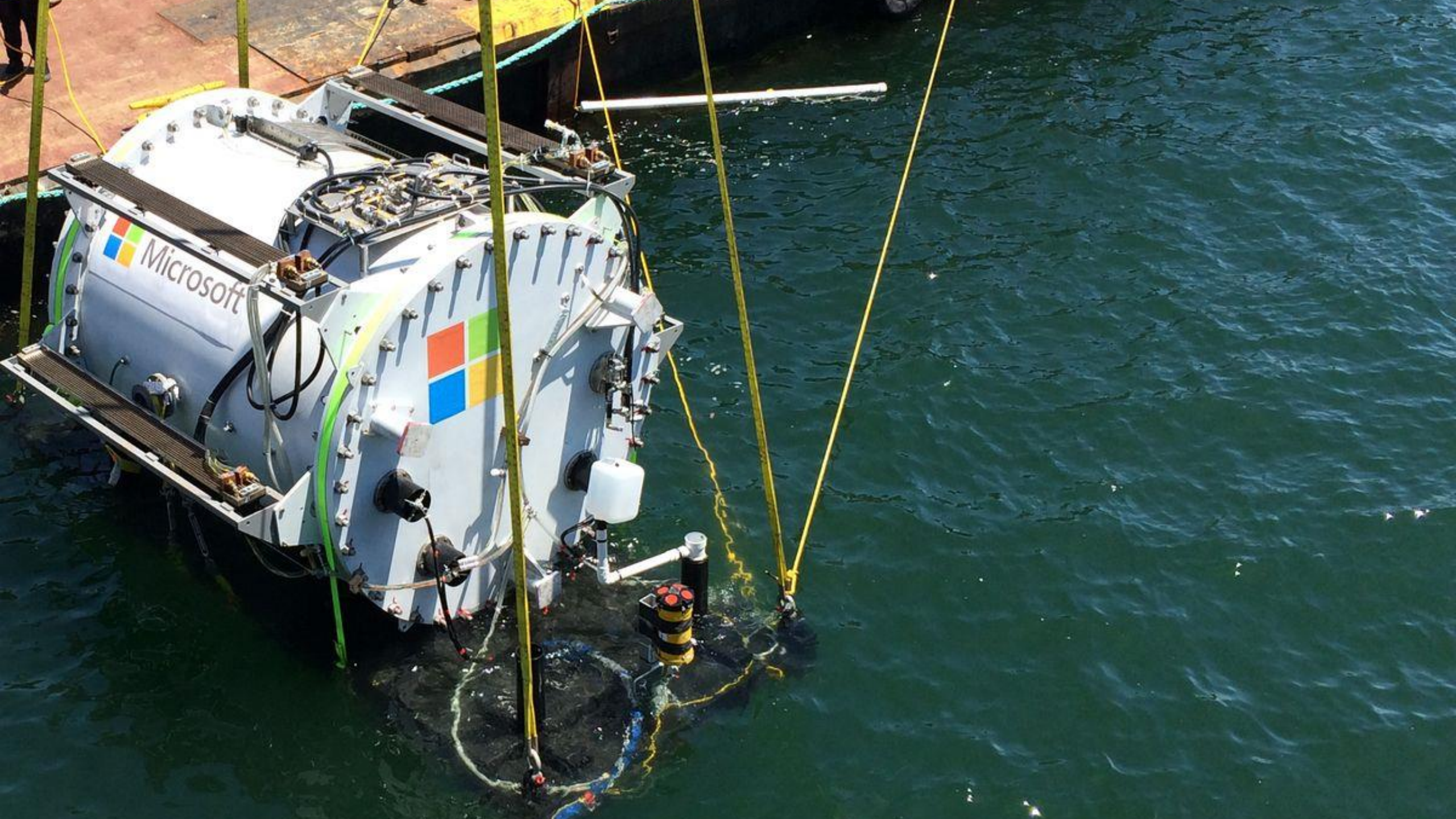
Diagnose & Visualize Scenarios with Network Watcher



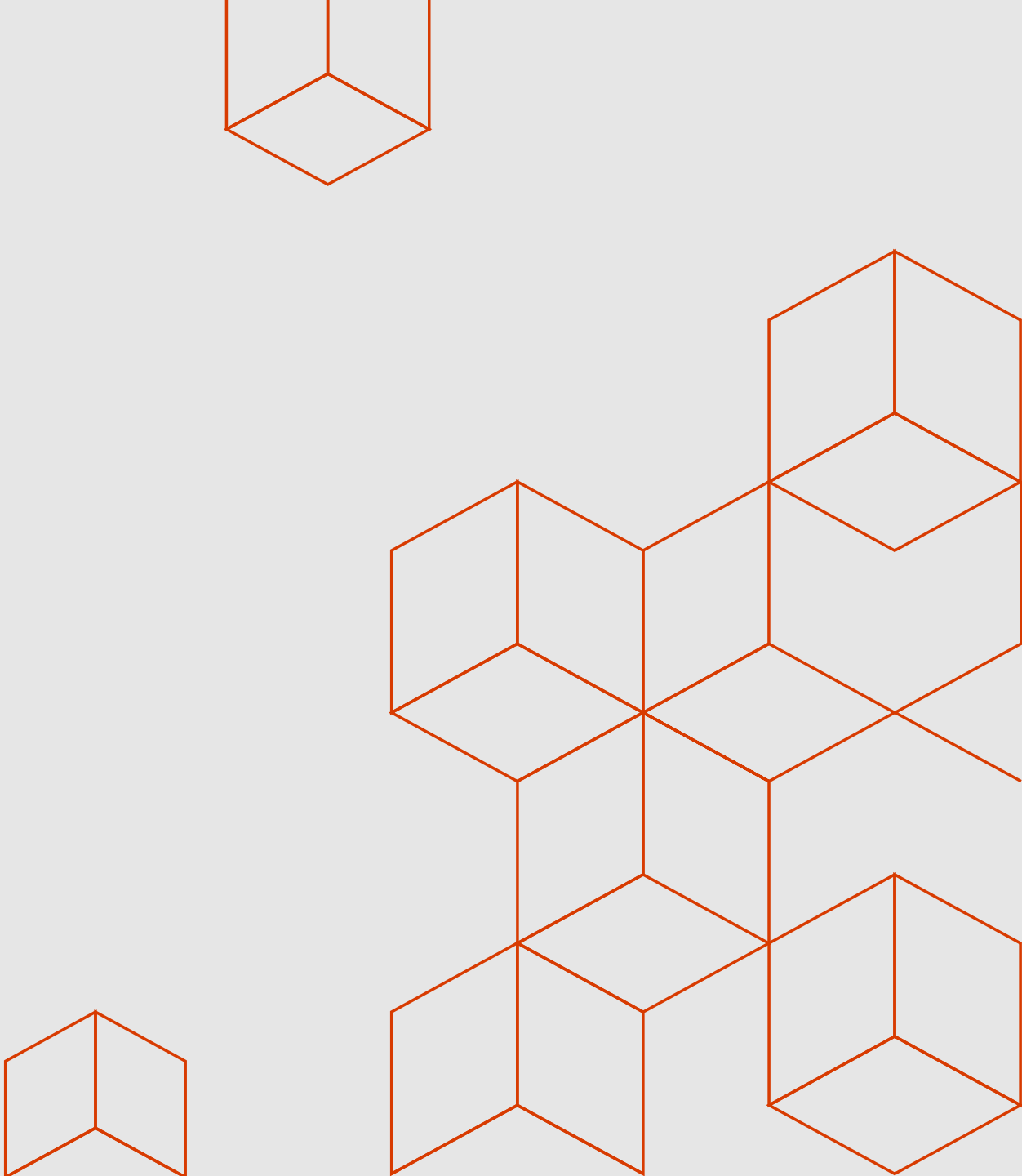
Planet-scale monitoring to optimize connectivity

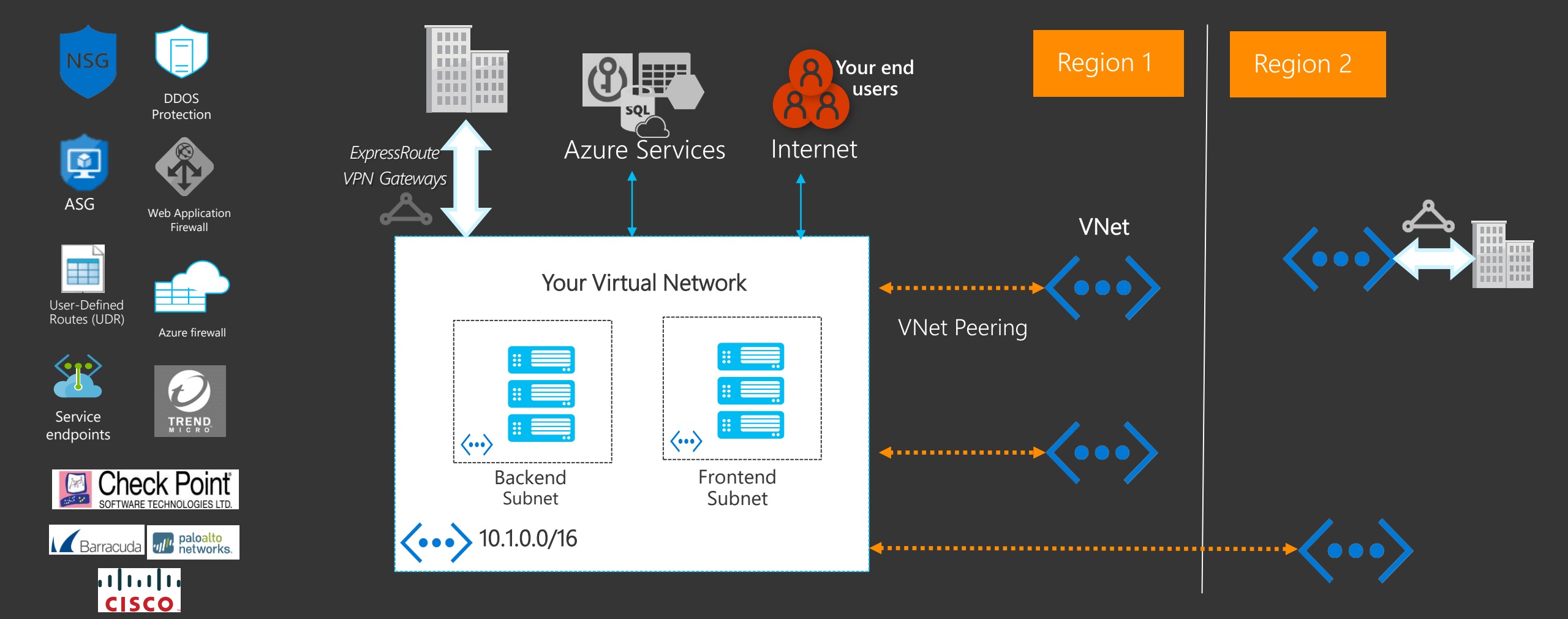



Microsoft


Microsoft

Network security challenges in the cloud

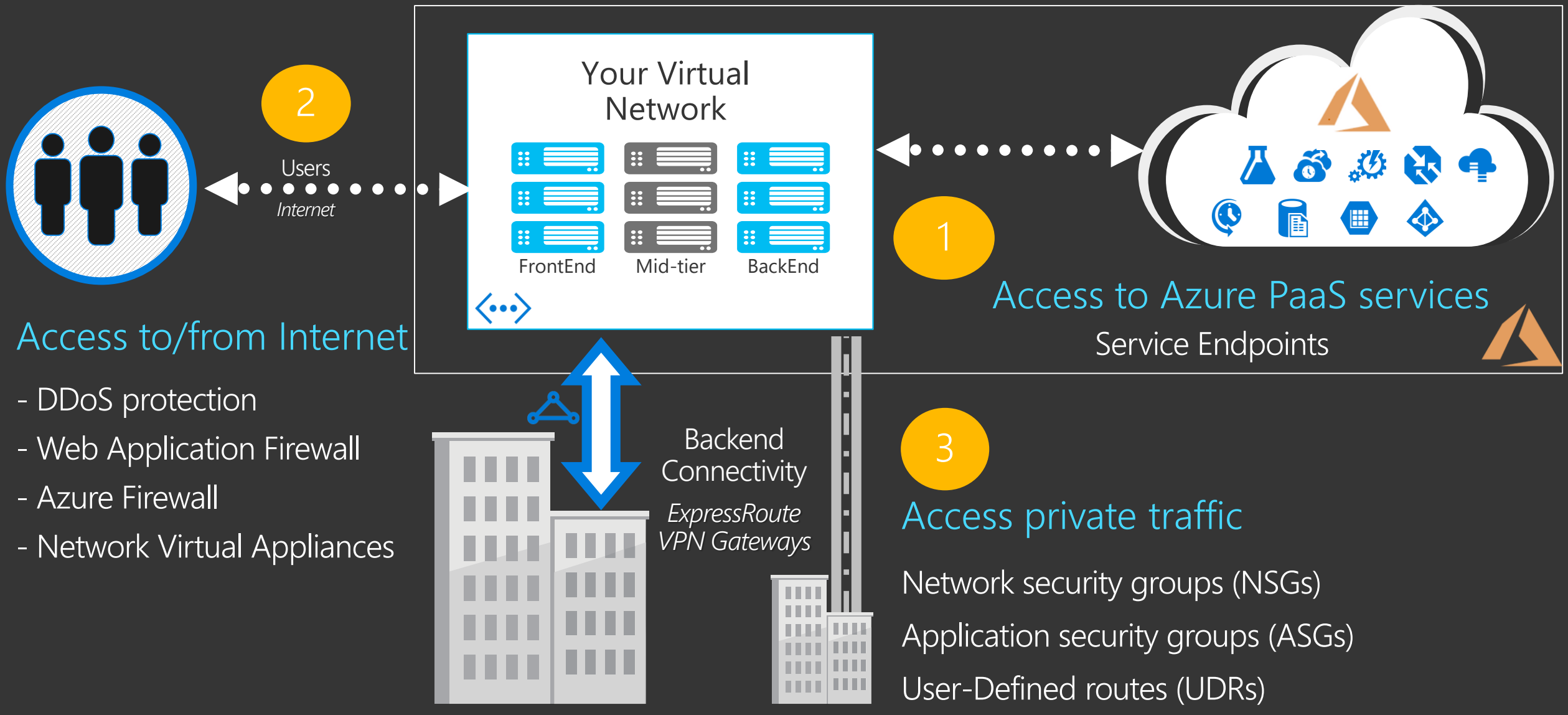




Planning network security in Azure

Similar controls as on-premises
Pick your network security offerings
Layer and scale

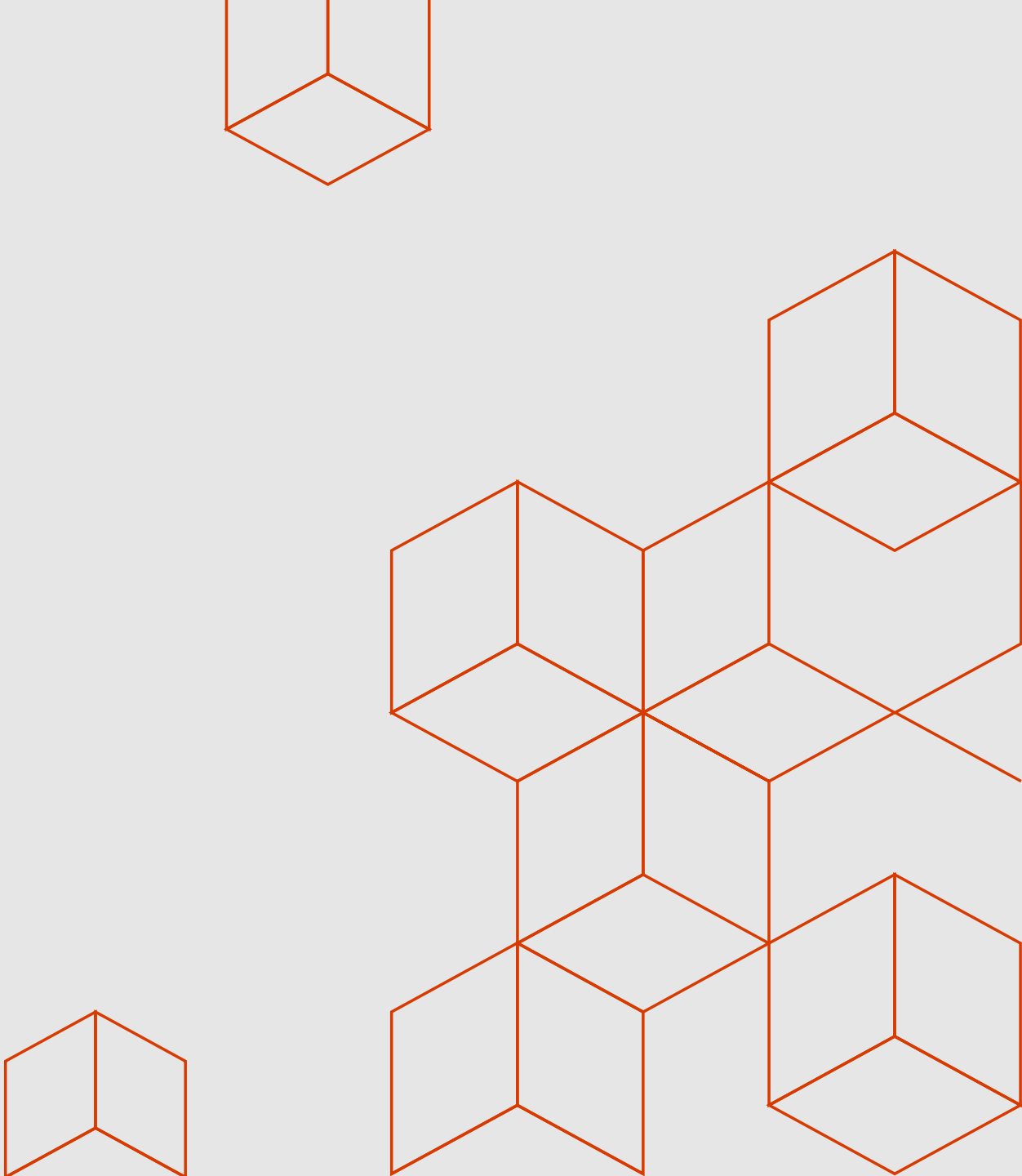
Application Access Patterns



Access to/from Internet

- DDoS protection
- Web Application Firewall
- Azure Firewall
- Network Virtual Appliances

Access Pattern 1: Securing VNet access to Azure Services

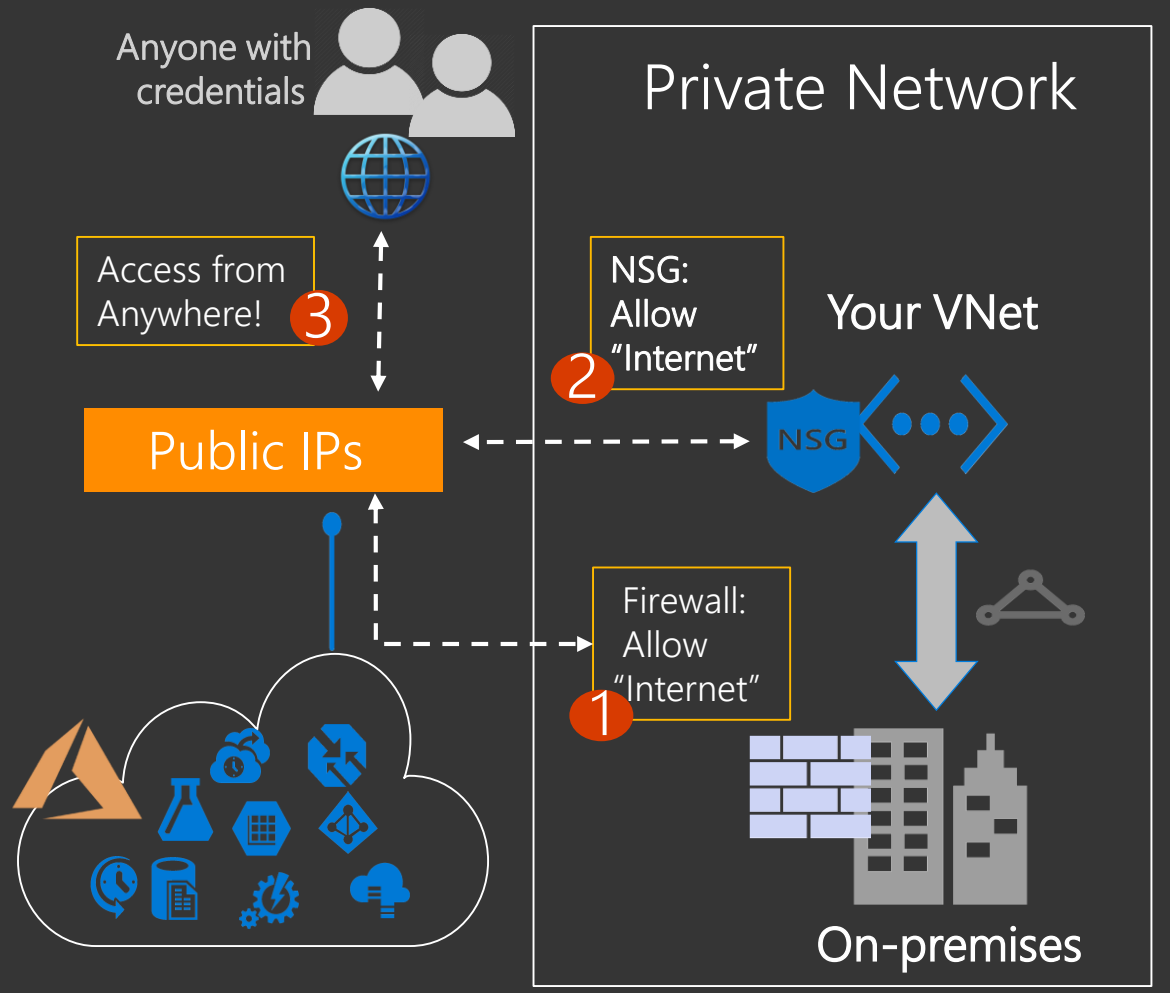


Security with Azure services

Azure service IPs reachable from anywhere!

Firewalls open to “Internet”

Application security not enough to prevent data leakage

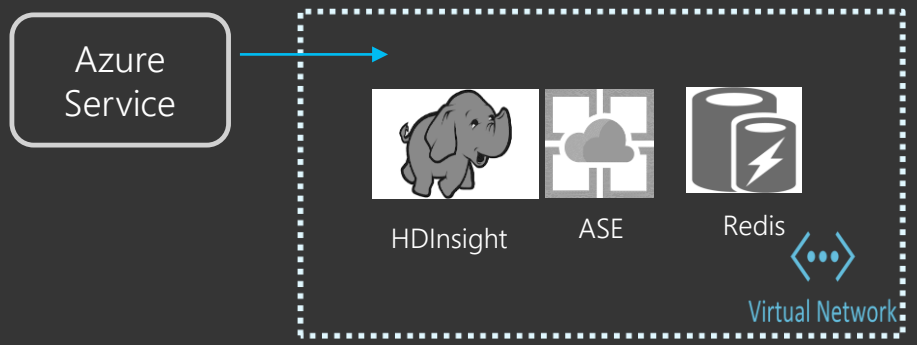


Private connectivity for services: Critical for network security

VNet-Azure Service Integration : Patterns

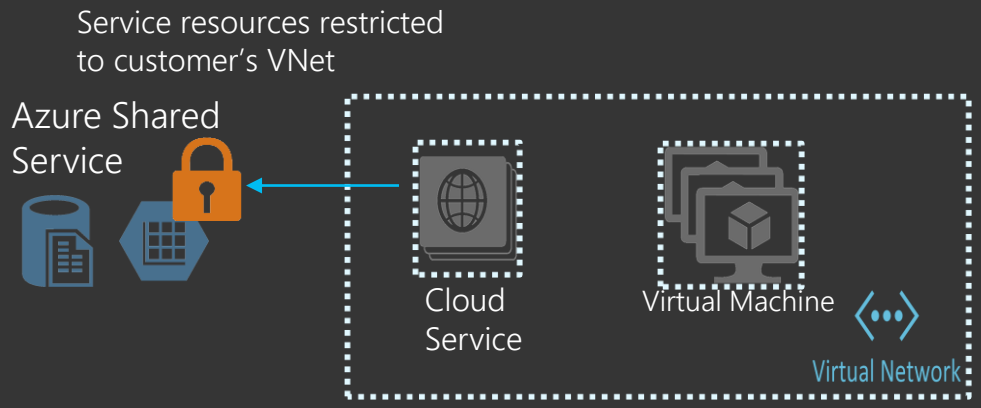
Pattern 1

Dedicated service instances in VNets



Pattern2

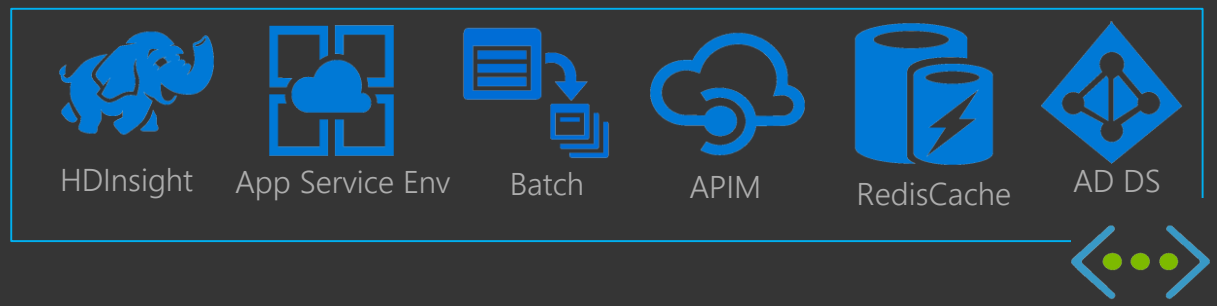
Extend VNets to shared, multi-tenant services



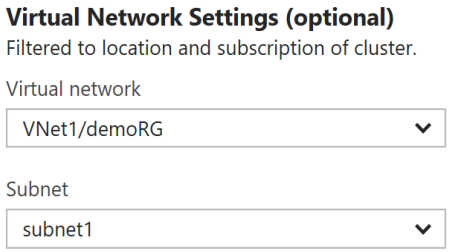
Pattern1

Deploy Azure services into VNet

- ✓ Services in your VNet, managed by Azure!
- ✓ Private IPs for service resources
- ✓ On-premises through Site-to-Site or ER private peering

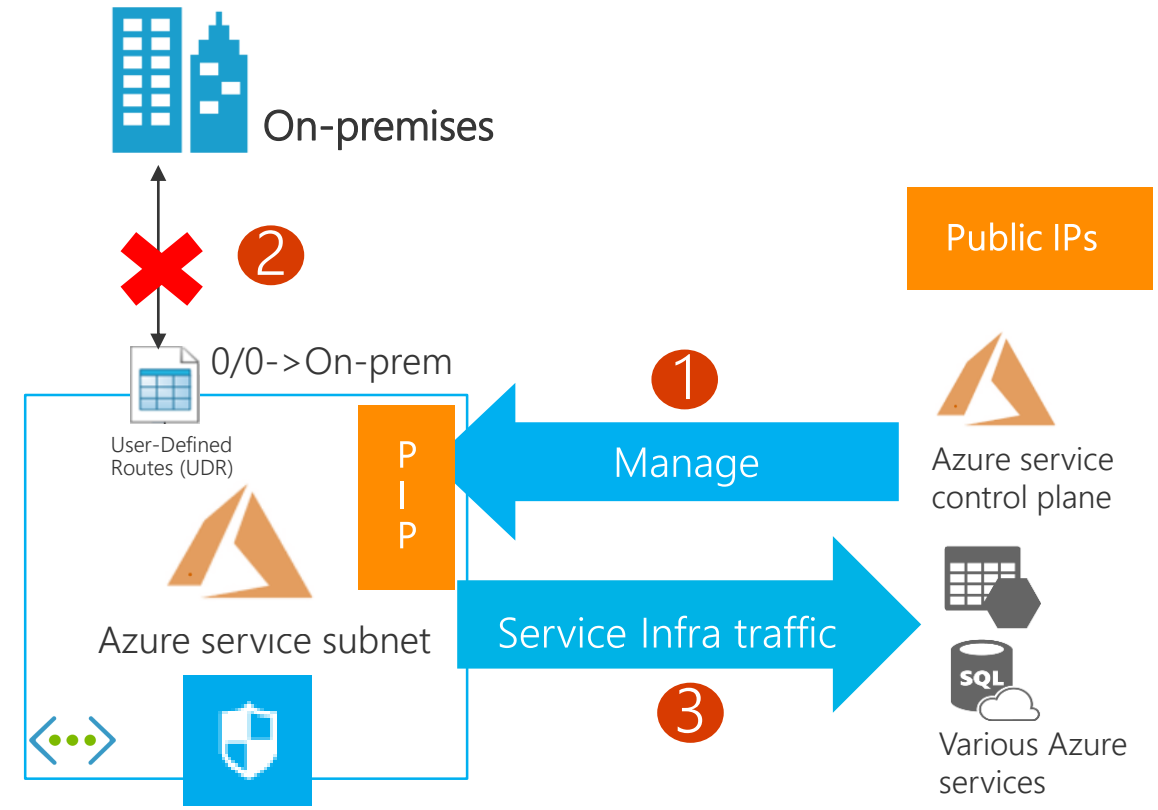


Azure Portal :
Service workflow



Securing Azure service traffic deployed in VNet

- Inbound or outbound IPs + ports open for management traffic
- Some services do not support force-tunneling or filtering via NVAs
- Services need outbound access to other Azure services for infra needs



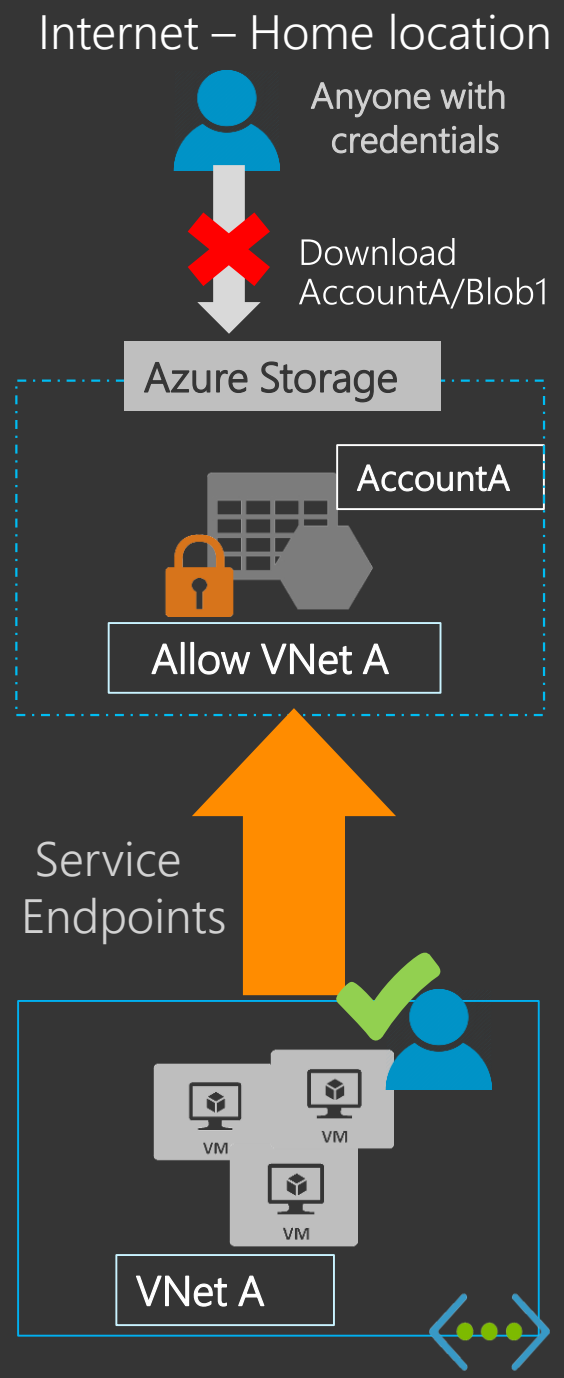
Network Security Group				
Action	Direction	Name	Source	Destination
Allow	Inbound	Allow "Manage" traffic	ServiceManagement	Virtual_Network
Allow	Outbound	Allow Azure services	Virtual_Network	Storage, SQL etc.
Deny	Outbound	Internet	*	Internet

Use NSG service tags to help reduce IPs and ports open

Pattern 2

VNet Service Endpoints

- Extend VNet identity to the service
- Secure your critical Azure resources to only your VNet
- Traffic remains on the Microsoft backbone

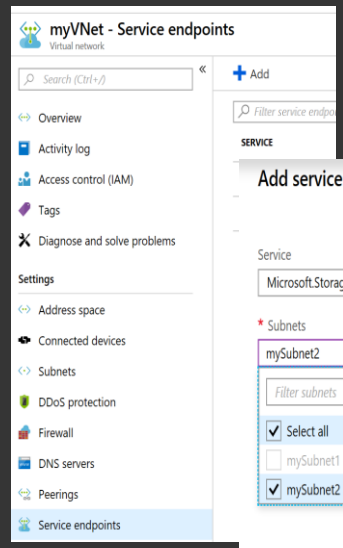


Azure services available on Service Endpoints

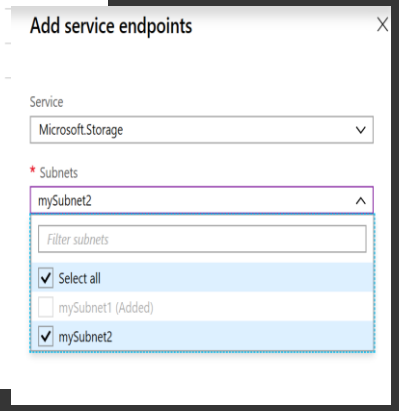
Azure Storage
Azure SQL Database
Azure SQL Data Warehouse
Azure CosmosDB
Azure Database services for PostgreSQL
Azure Database services for mySQL
Azure Database services for MariaDB
Azure Key Vault
Azure Event Hubs
Azure Service Bus
Azure App Service
Azure Data Lake Store Gen 1
Azure Container Registry *(Preview)*

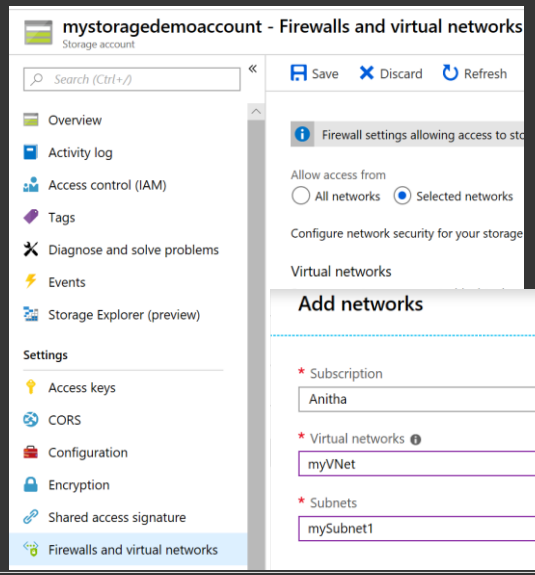
How to secure your resouces for one-time migration?

Normal Flow



Step 1: Set Endpoint on your subnet

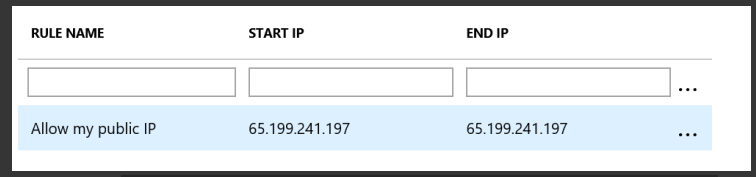




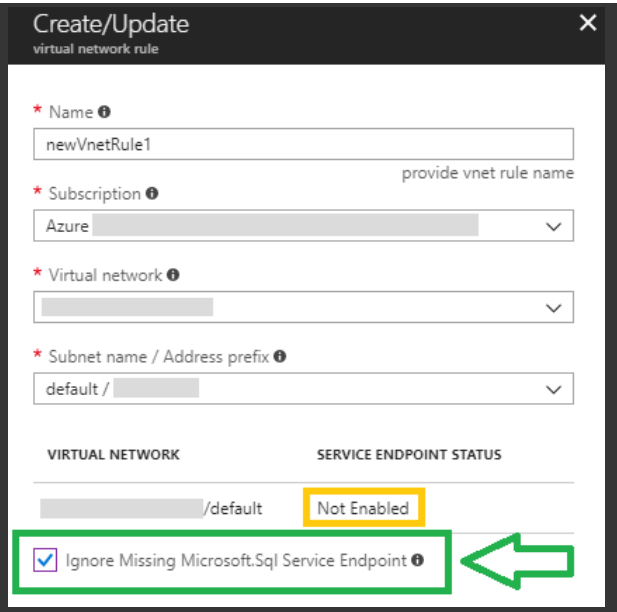
Step 2: Lock your service resource to your subnet

One-time migration: If you have existing public IP firewall

Setting service endpoint changes source IP to private! Ensure connectivity:



Step 1: Add VNet rule without Endpoint



Step2: Set endpoint on subnet
Step3: Remove the public IP setting

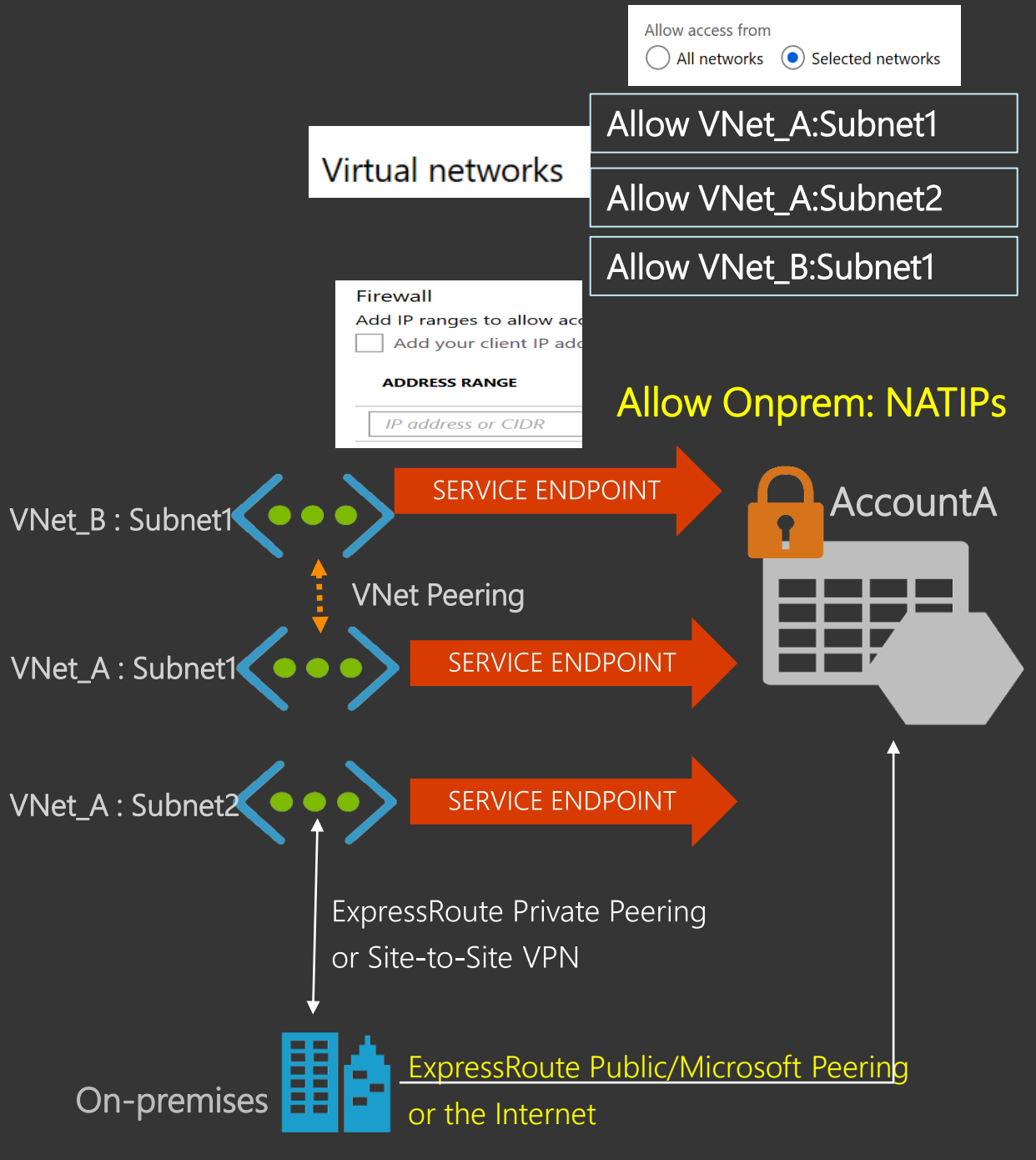
Remove “Allow All Azure services” or “Allow All” settings

Service endpoints: Scaling security

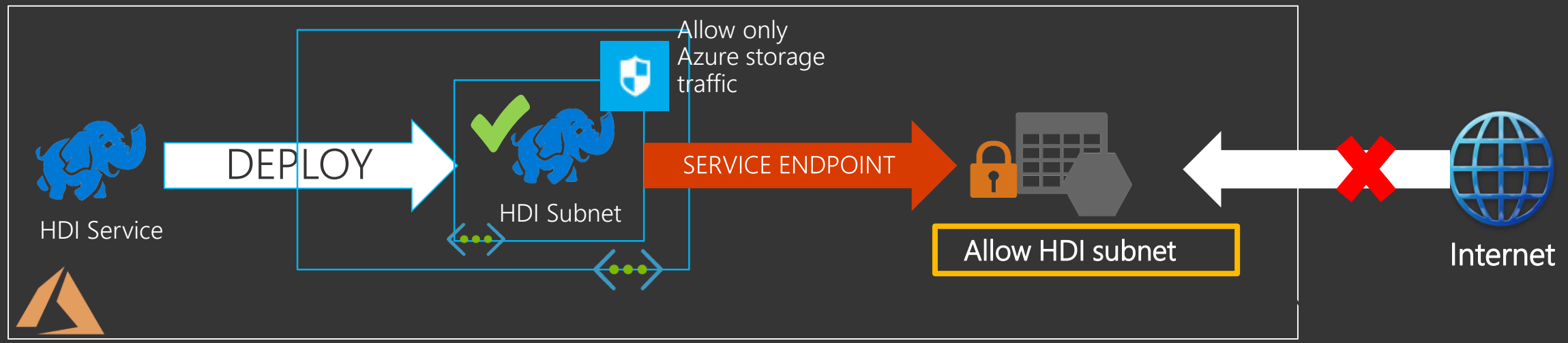
- Resource locked to a VNet:
  No access to other VNets or Internet or on-premises.

- Permit more VNets:
  Turn on service endpoints on VNets
  and
  add under “Virtual Networks” on resource

- Permit on-premises:
  Add the on-prem NAT IPs under “Firewall” on resource



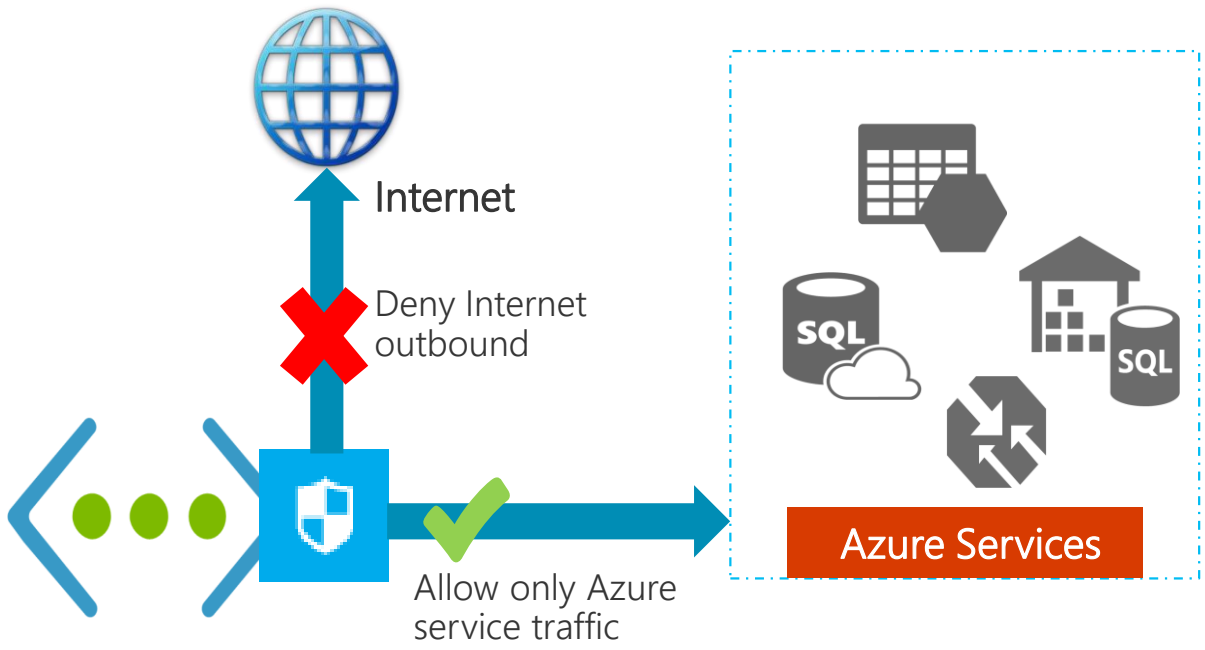
Stitching Azure services together



- Secure Azure resources to managed service subnets with endpoints
- Applies to all services directly deployed into VNet

Securing VNet traffic: Service Tags in NSGs

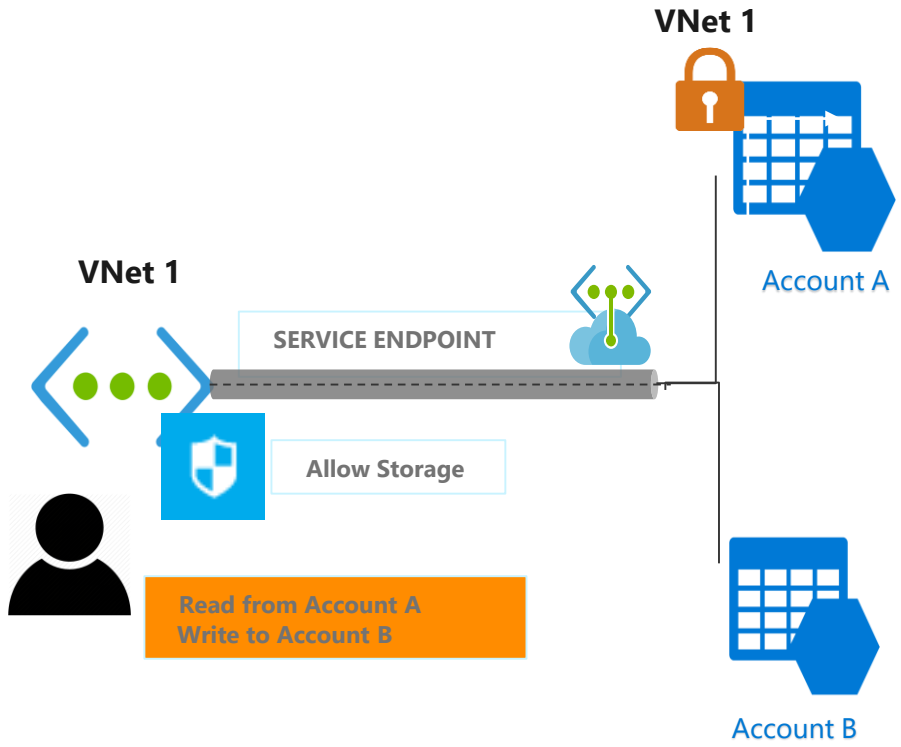
- Restrict network access to just the Azure services you use.
- Maintenance of IP addresses for each tag provided by Azure
- Support for global and regional tags (varies by service)



Network Security Group (NSG)				
Action	Name	Source	Destination	Port
Allow	AllowStorage	VirtualNetwork	Storage	Any
Allow	AllowSQL	VirtualNetwork	Sql.EastUS	Any
Deny	DenyAllOutBound	Any	Any	Any

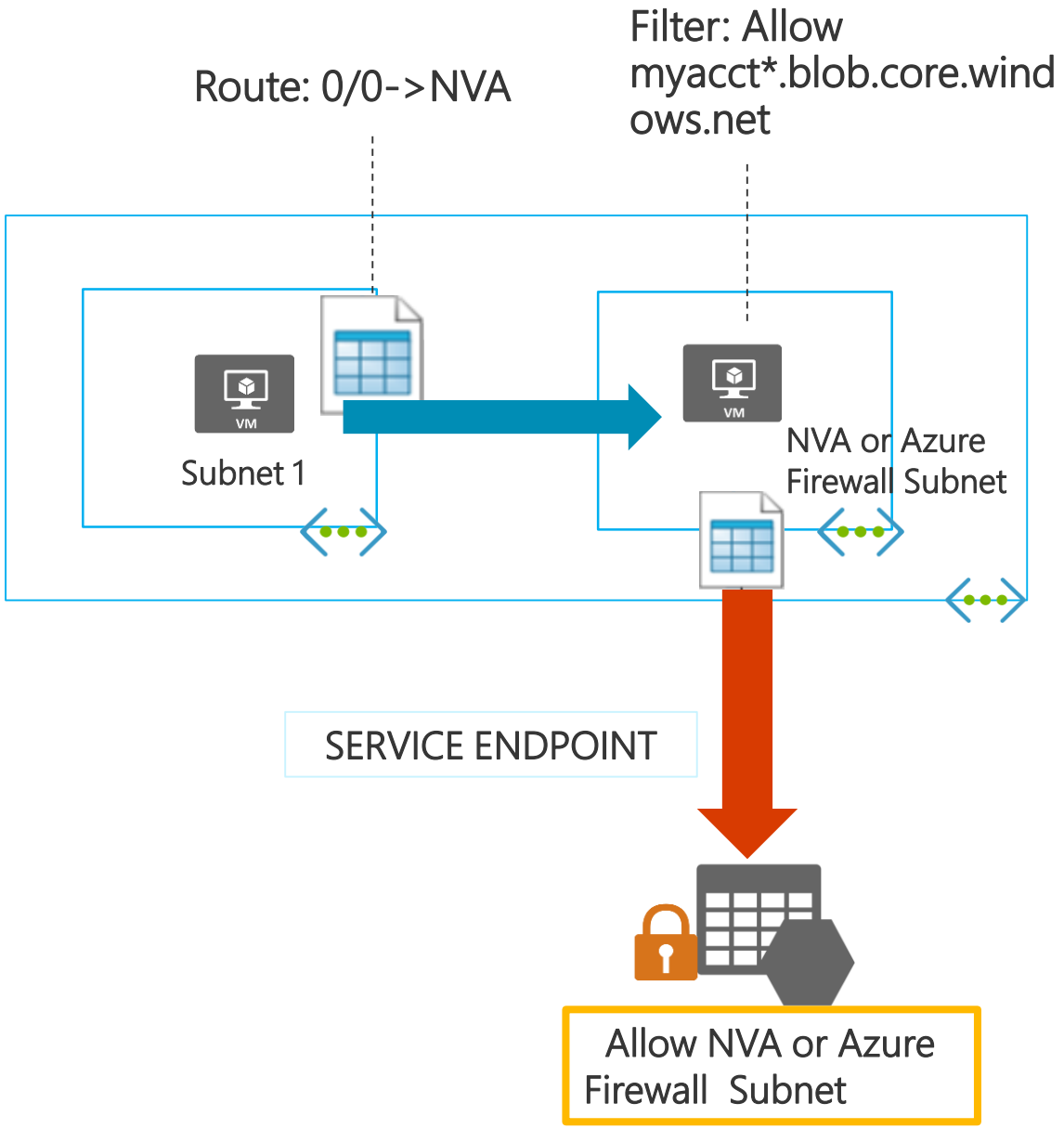
Service Endpoints: Data-Exfiltration risk

- NSG Service tags not enough to prevent data-exfiltration from VNet
- Access to unauthorized accounts possible!



Service Endpoints: Filter service traffic with appliance

- Service endpoints bypass NVAs for service traffic, if set on originating subnet
- Optionally, continue using NVAs for auditing/filtering service traffic
- Set endpoint on NVA subnet instead and secure resouces to that subnet

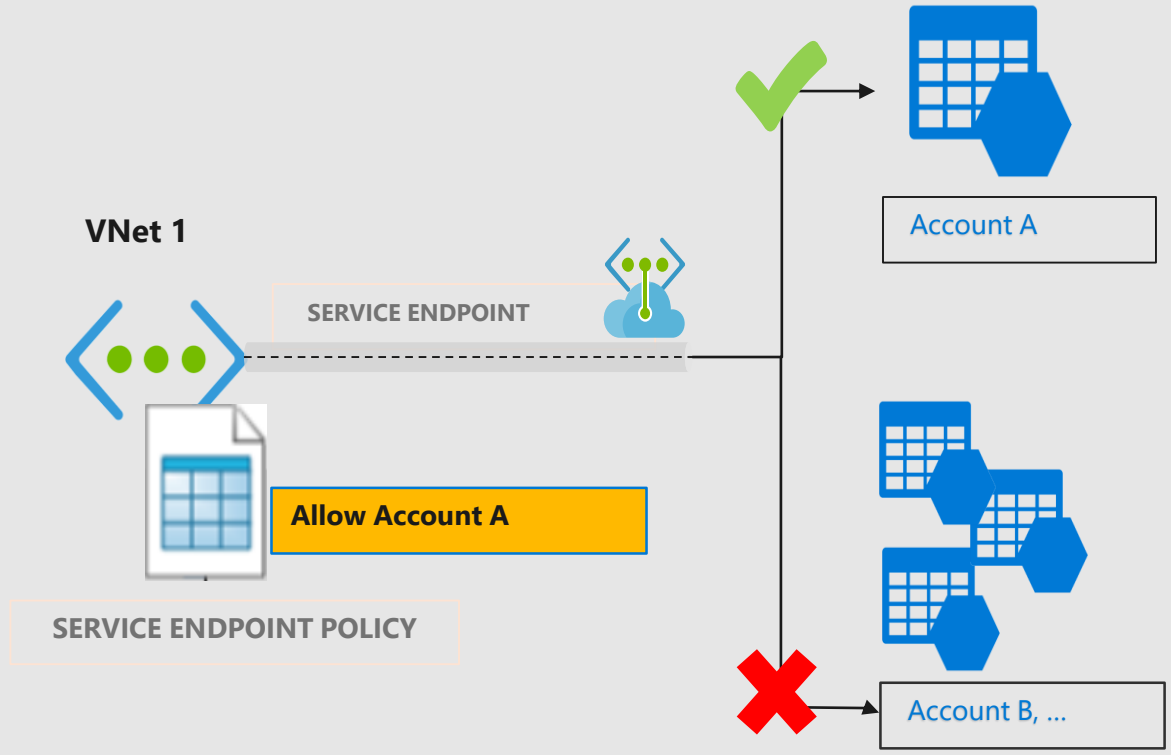


Service Endpoints Policies

Enhanced VNet security for Azure services

Preview

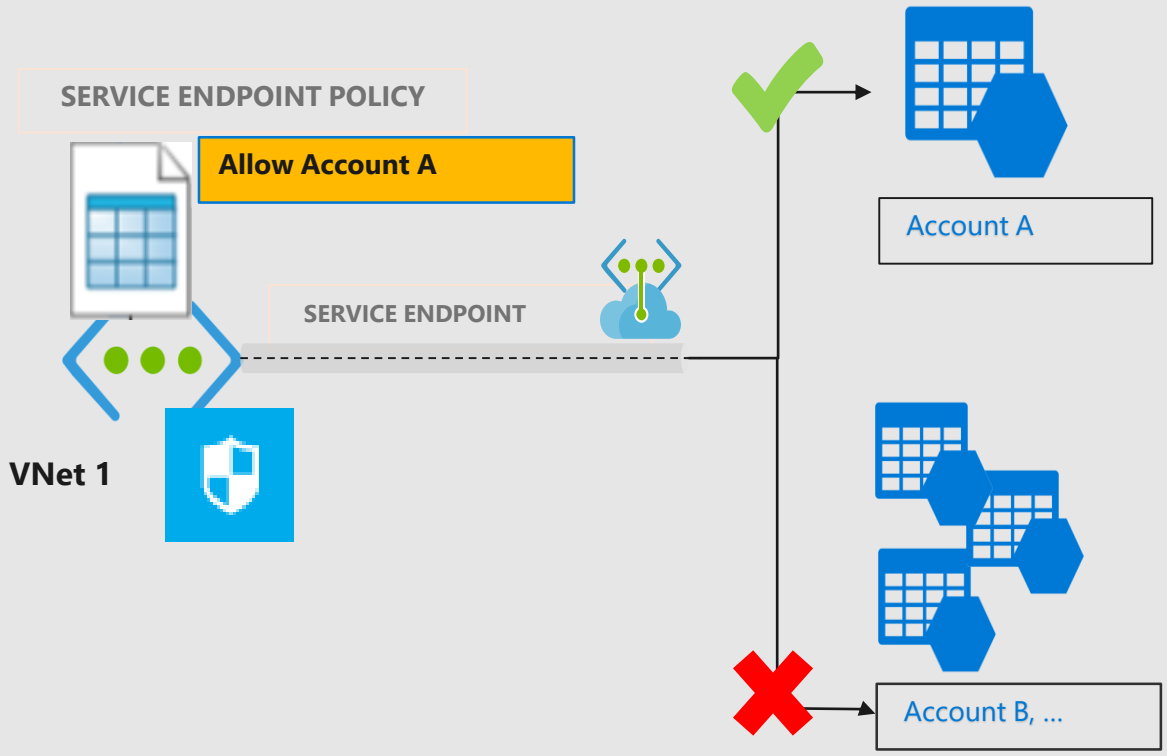
- Prevent unauthorized access to storage accounts
- Restrict Virtual Network access to specific Azure Storage Accounts
- Granular access control over service endpoints



Azure Storage: West Central US and West US2

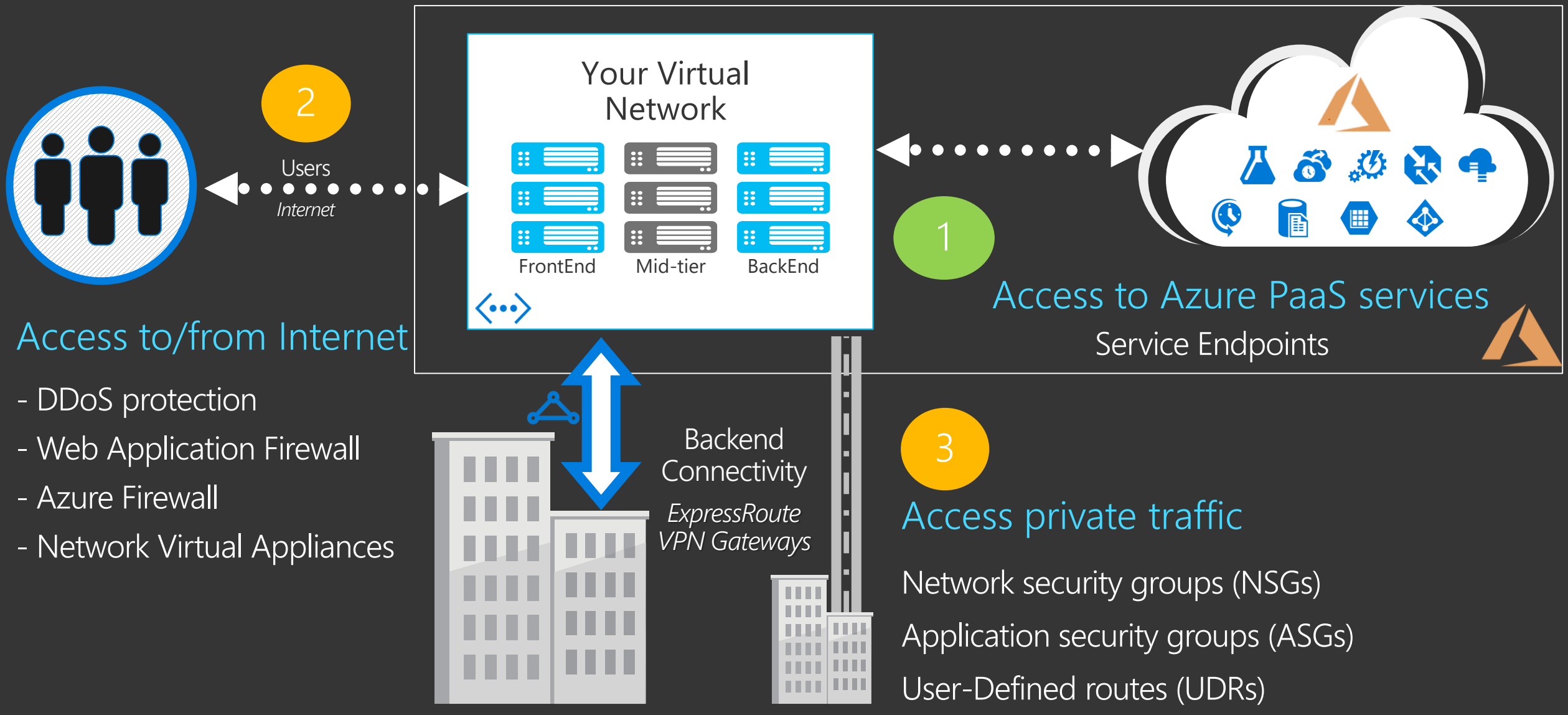
Layering NSGs with endpoint policies

- Service endpoint policies will only filter traffic for endpoint regions
- If NSGs are open wider, accounts in other regions can be accessed from VNet
- Layer policies with NSGs set to allow only endpoint region service tags for Storage



Network Security Group (NSG)				
Action	Name	Source	Destination	Port
Allow	Allow Storage	VirtualNetwork	Storage.WestCentralUS	Any
Allow	AllowSQL	VirtualNetwork	Storage.WestUS2	Any
Deny	DenyAllOutBound	Any	Any	Any

Application Access Patterns



Access to/from Internet

- DDoS protection
- Web Application Firewall
- Azure Firewall
- Network Virtual Appliances

Access Pattern 2: Securing access from Internet

Potential threats

DDoS Attacks

How to protect my internet exposed workloads from DDoS attacks?

Web Application vulnerabilities

How to prevent exploit of common vulnerabilities on my web applications?

DDoS Defense

DDoS protection

Designed into the global network

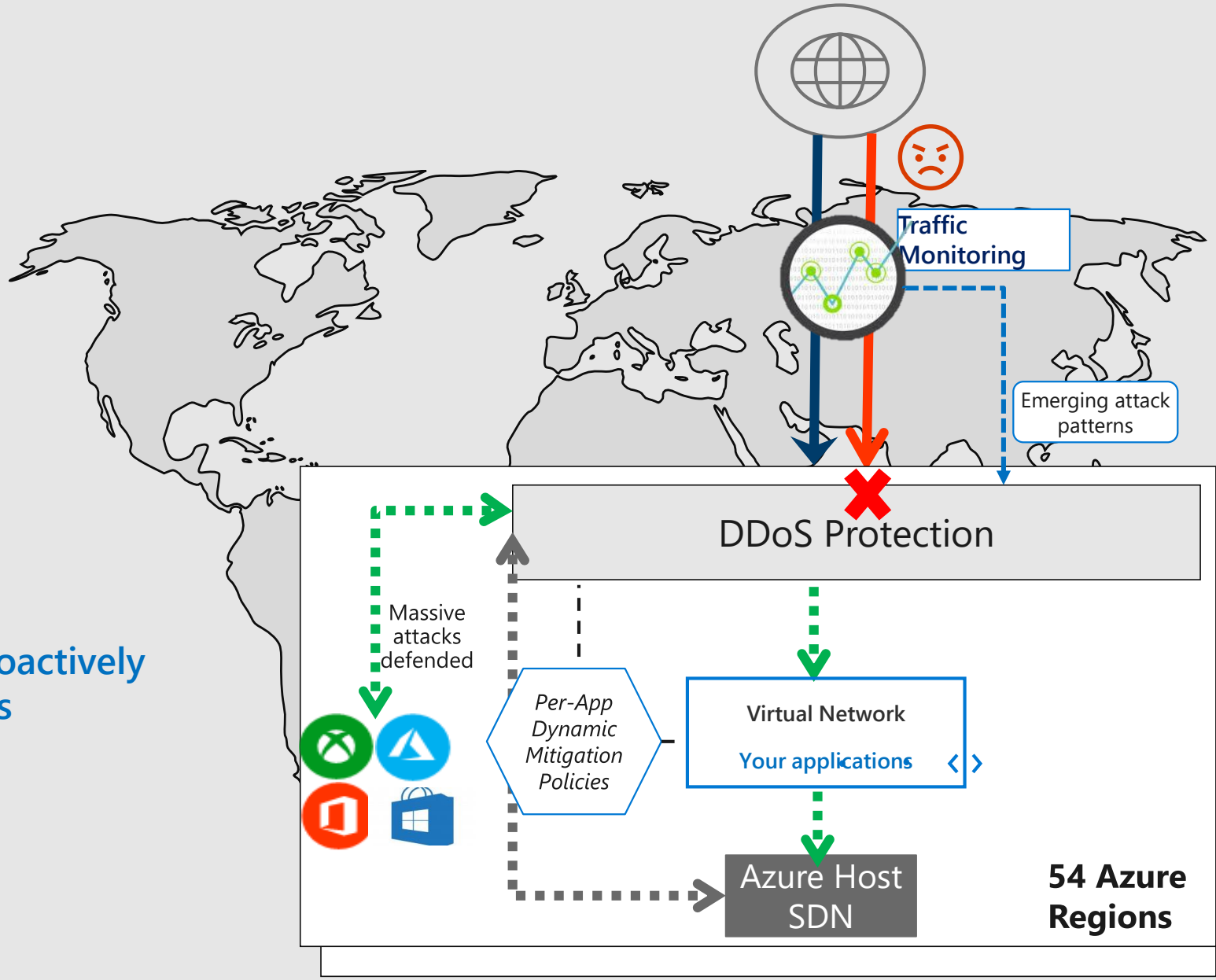
Global distribution of the attack during large scale attacks

25+ Tbps global mitigation capacity

Continuous monitoring and learning to proactively detect emerging threats and attack vectors

Proven defense for Microsoft Services

Specifically tuned protection for you app



Azure DDoS Protection

Cloud scale DDoS protection tuned to applications

GA

What's new

DDoS Attack Analytics

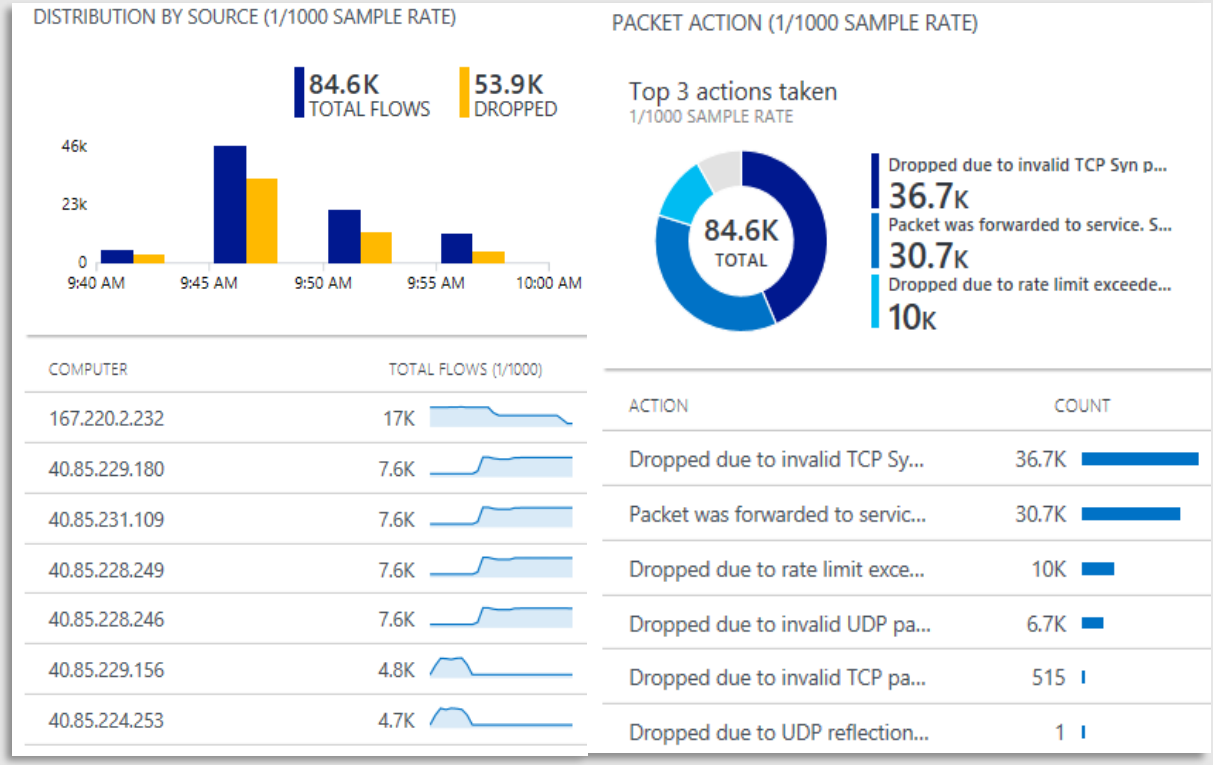
- Near real time network attack mitigation flow logs
- Attack data snapshots and full post attack summary

DDoS Rapid Response

- Specialized Rapid Response team support during active attacks
- Custom mitigation policy configuration

Azure Security Center integration

- Intelligent DDoS Protection virtual network recommendation



Attack flow logs Azure Log Analytics view

Web Application Firewall

Platform managed built in high availability and scalability
Layer 7 load balancing URL path, host based, round robin, session affinity, redirection
Centralized SSL management SSL offload and SSL policy
Public or ILB public internal or hybrid
Rich diagnostics Azure monitor, Log analytics

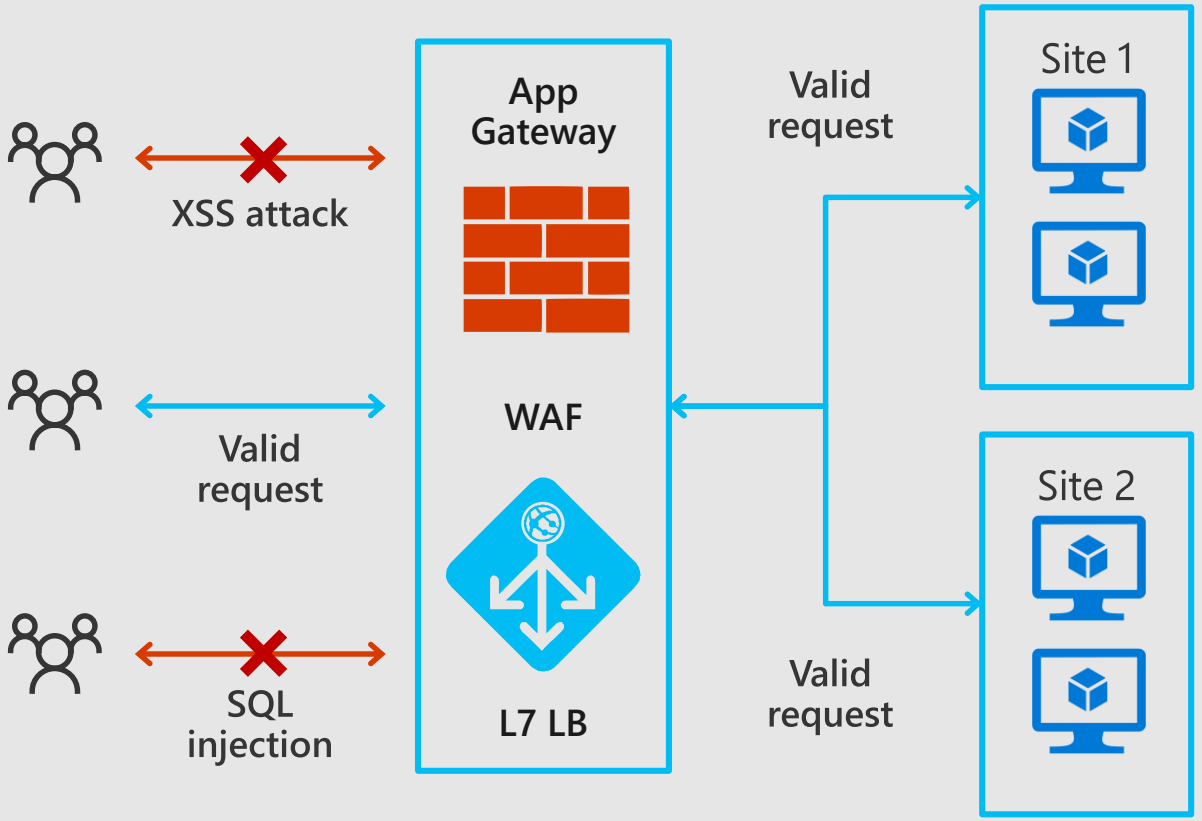
Web application protection

Protects your application against prevalent X-Site Scripting and SQL Injection attacks

Blocks threats based on top 10 OWASP signatures

Integrated with Azure Security Center

Real-time logging with Azure Monitor



Application Gateway - WAF

Preview

Layer 7 load balancer for web applications

What's New

Features
Connection draining support & Custom error pages
Ingress Controller for Azure Kubernetes Service (AKS) preview

Diagnostics
Enhanced multi dimensional metrics
Diagnose connectivity issues with Network Watcher integration

Portal enhancements
SSL policy, VMSS, Web App Services, Custom error pages, Redirection, Connection draining

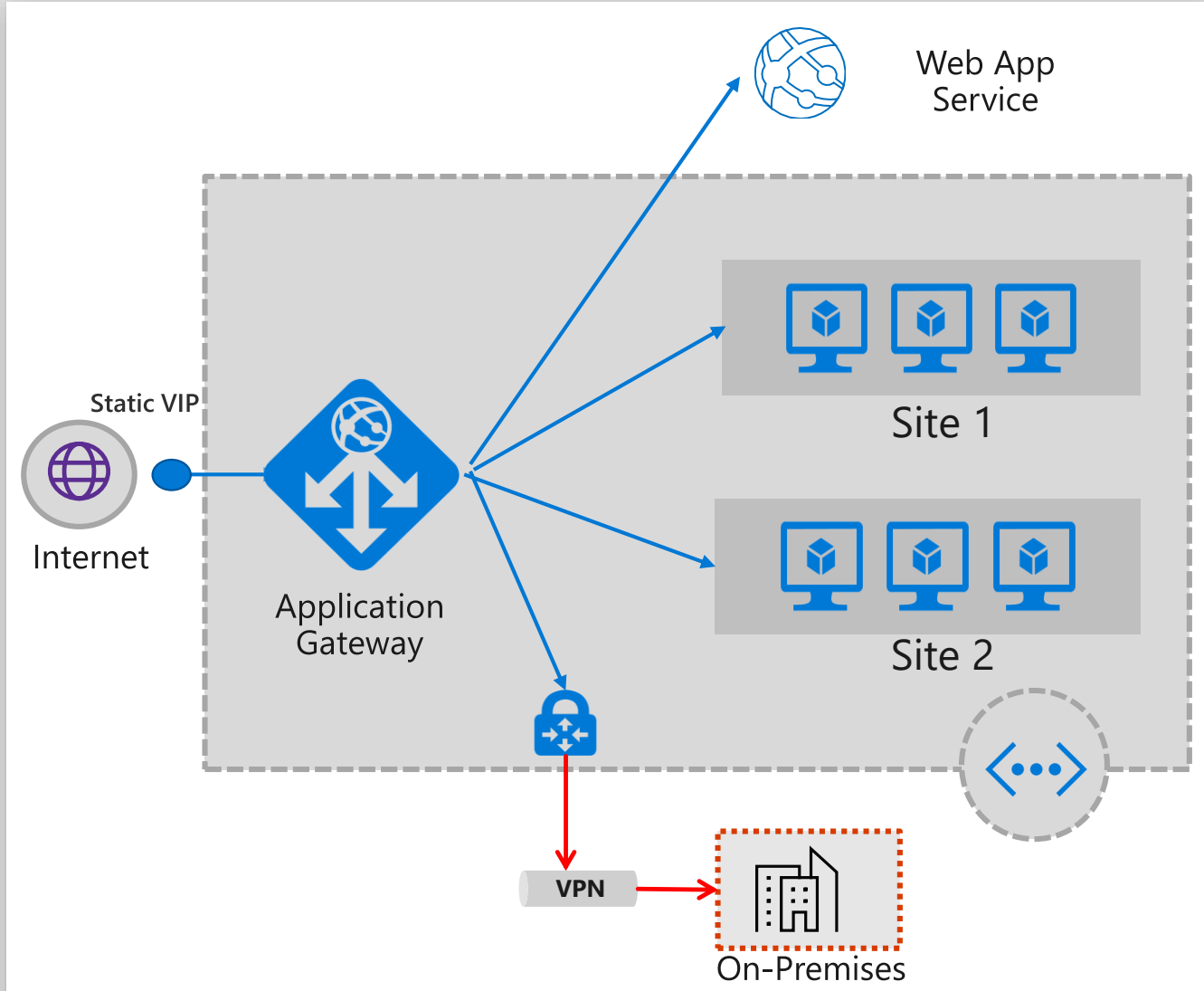
Autoscaling
Grows and shrinks based on application traffic requirements

Better performance 5X better SSL offloads

Faster provisioning and configuration update

Enhanced resiliency
Built in Azure zone redundancy

Feature enhancements
Robust Application Gateway IP static VIP
More features upcoming (Key Vault integration, modify headers)



Recap of security options- Protection from Internet

Securing Access From Internet

DDoS Protection for public IP addresses

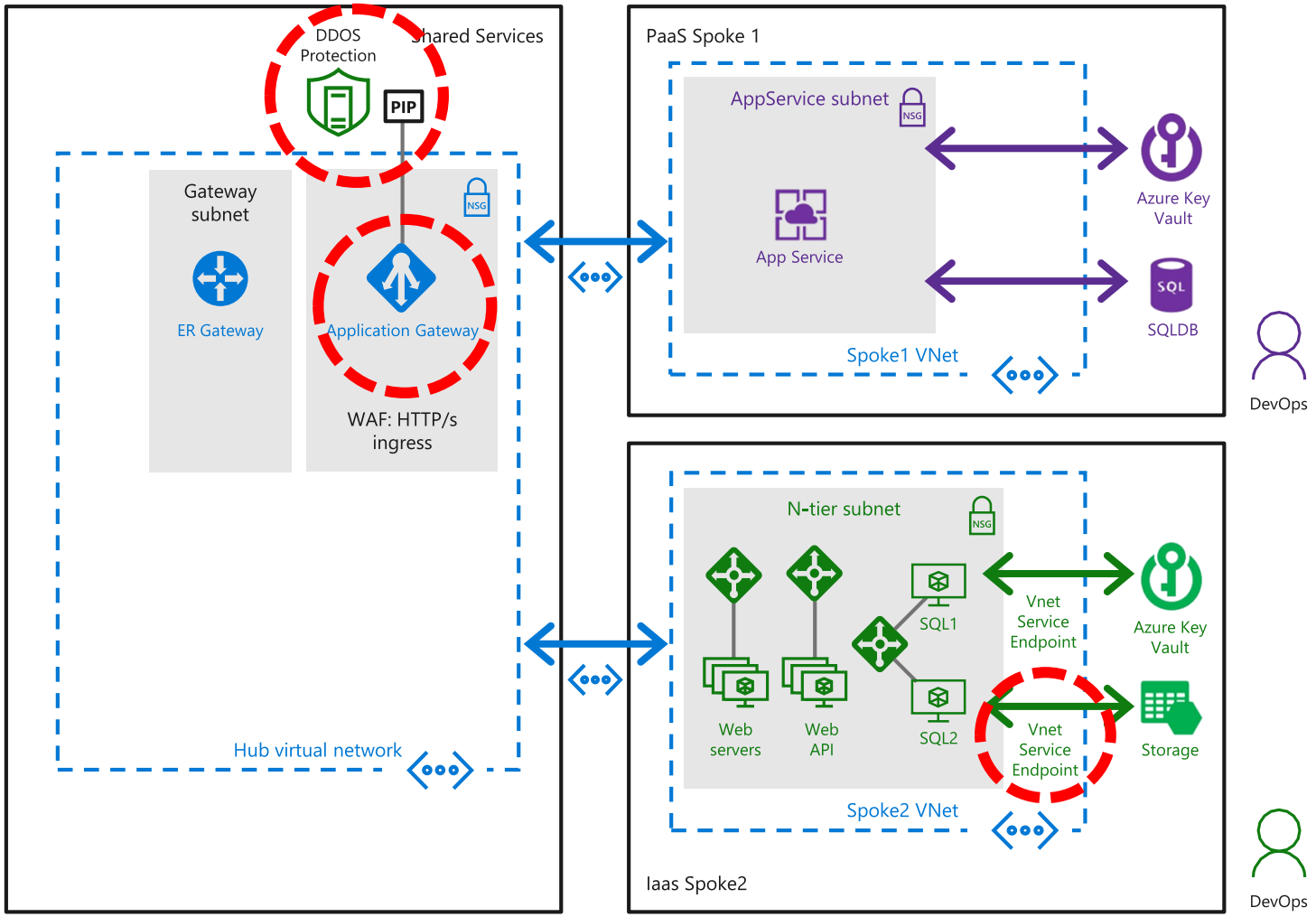
Intelligent DDoS Protection

Application Gateway/Web Application Firewall

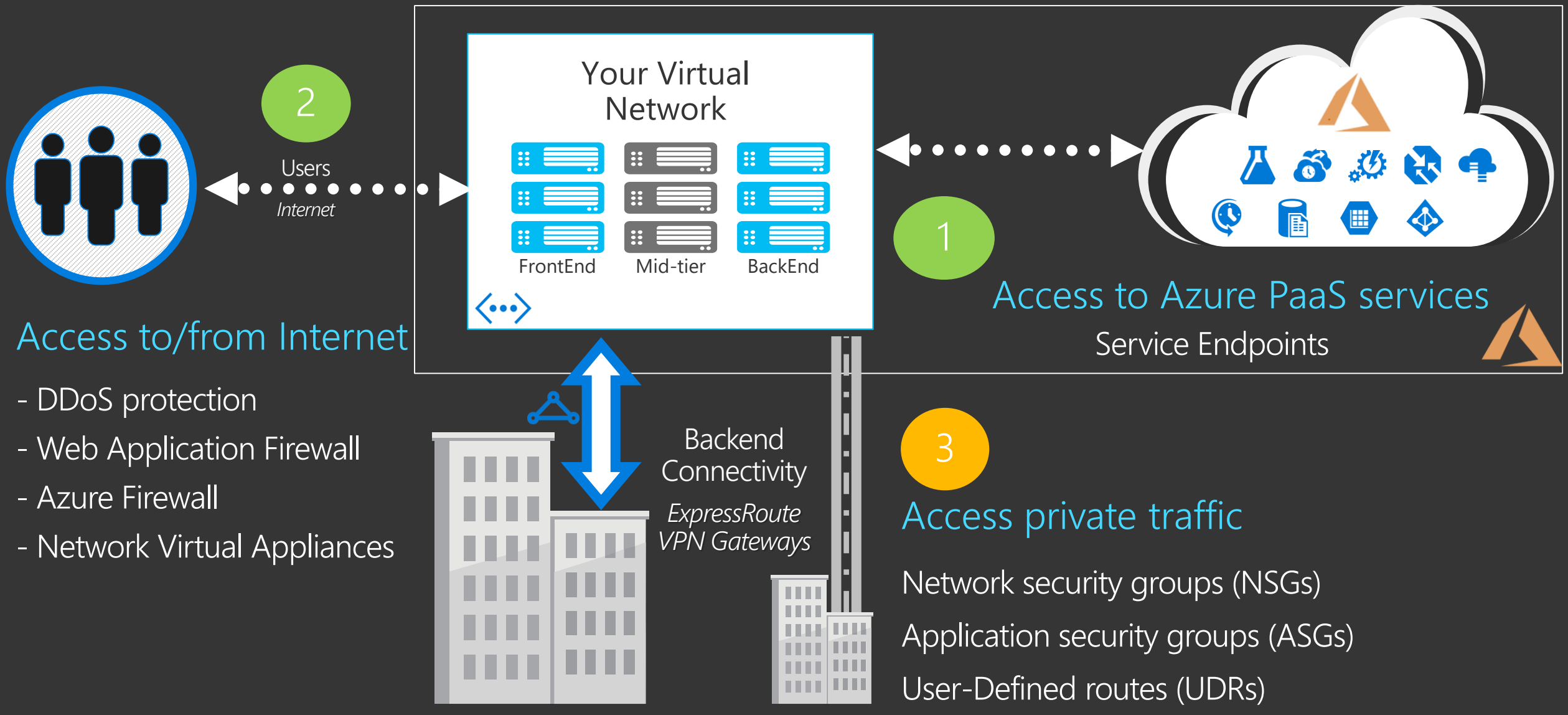
Web application protection

Service Endpoints

Azure PaaS resource protection



Application Access Patterns



Access to/from Internet

- DDoS protection
- Web Application Firewall
- Azure Firewall
- Network Virtual Appliances

Securing access from my Virtual Network

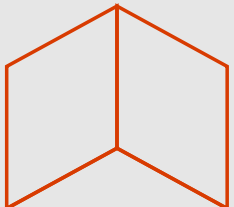
Potential threats

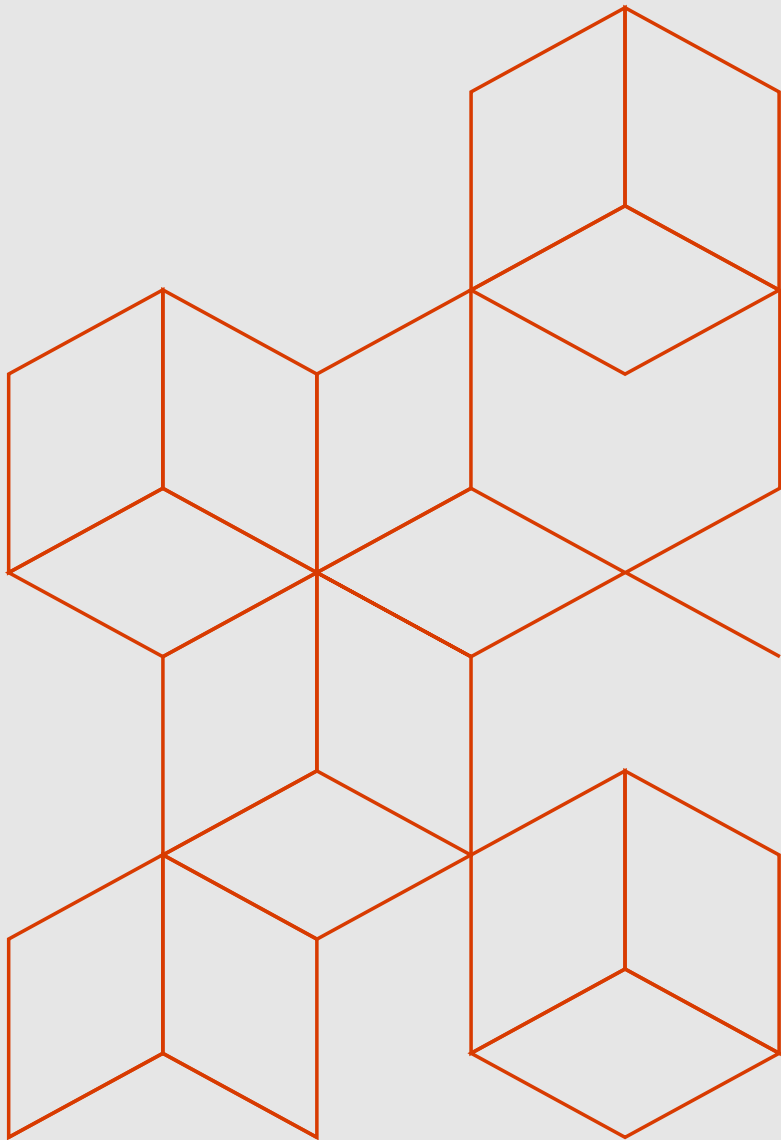
Unrestricted inbound traffic

How to prevent access from DMZ to private zones, other applications or on premises network?

Unrestricted outbound traffic

How to prevent access to untrusted destinations, downloads of malware, stealing data on the internet…?





Network and Application Security Groups

Network security for your VNet traffic

Network Security Groups

- Protects your workloads with distributed ACLs
- Simplified configuration with augmented security rules
- Enforced at every host, applied on multiple subnets

Application Security Groups

- Micro-segmentation for dynamic workloads
- Named monikers for groups of VMs
- Removes management of IP addresses

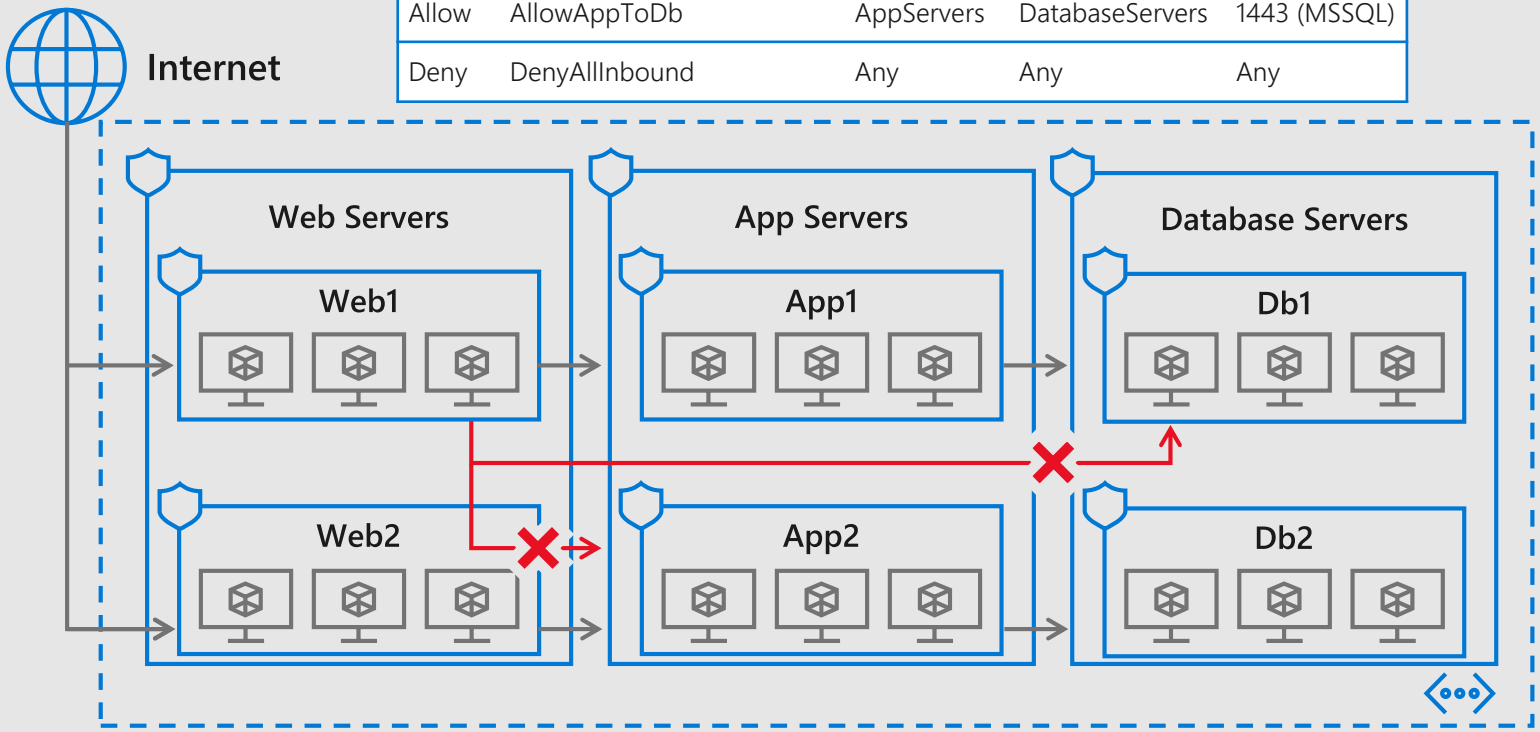
Service Tags

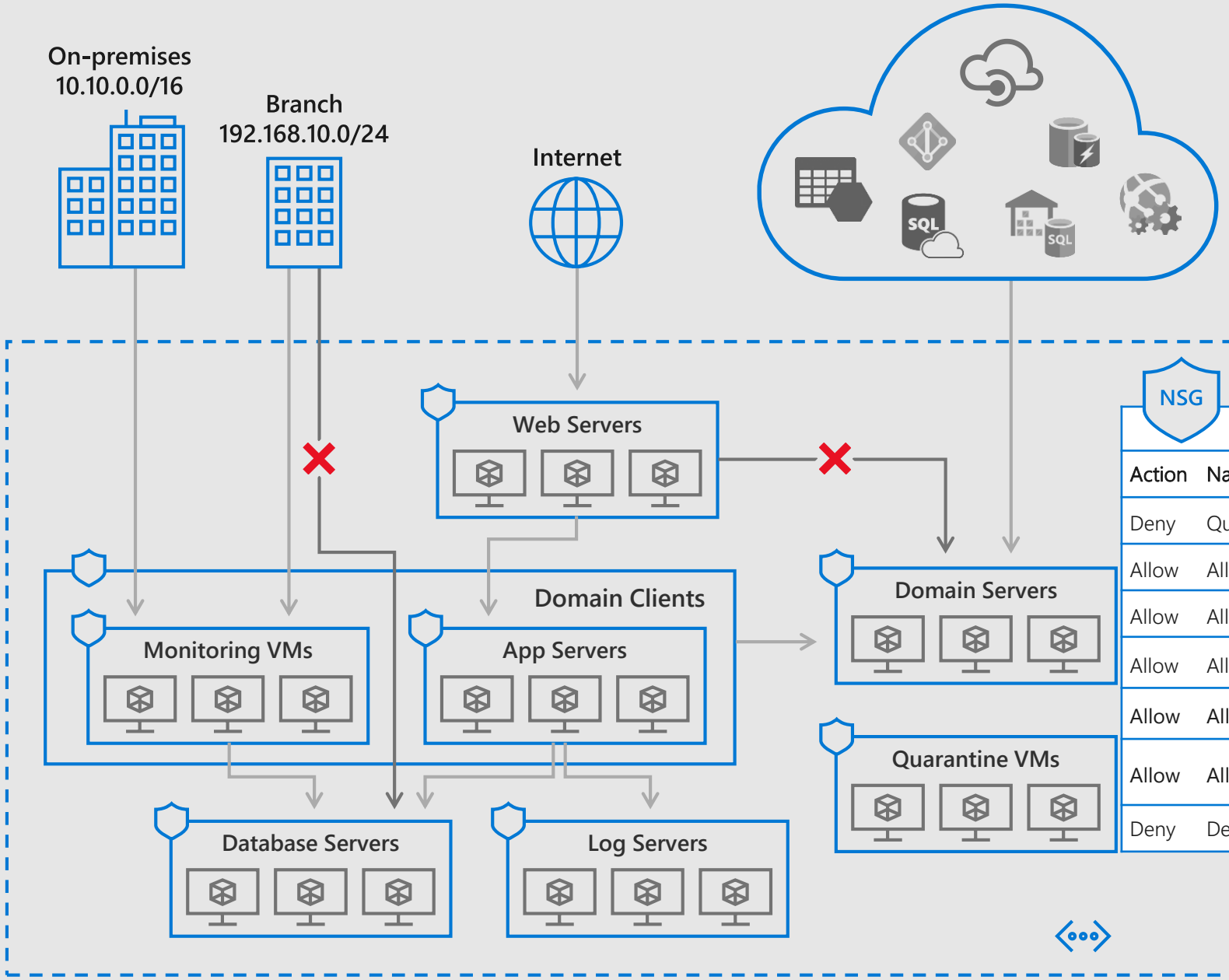
- Named monikers for Azure service IPs
- Many Services tagged including AzureCloud

Logging and troubleshooting

- NSG flow logs for traffic monitoring
- Integrated with Network Watcher
- JIT access policies with Azure Security Center

Network Security Group (NSG)				
Action	Name	Source	Destination	Port
Allow	AllowInternetToWebServers	Internet	WebServers	80,443(HTTP)
Allow	AllowWebToApp	WebServers	AppServers	443 (HTTPS)
Allow	AllowAppToDb	AppServers	DatabaseServers	1443 (MSSQL)
Deny	DenyAllInbound	Any	Any	Any





Network Security Group (NSG)

Action	Name	Source	Destination	Port
Deny	QurantineVMs	Any	QurantineVMs	Any
Allow	AllowInternetToWebServers	Internet	WebServers	80,443(HTTP)
Allow	AllowWebToApp	WebServers	AppServers	443 (HTTPS)
Allow	AllowAppToDb	AppServers	DatabaseServers	1443 (MSSQL)
Allow	AllowAppToLogServers	AppServers	LogServers	8089
Allow	AllowOnPrem	10.10.0.0/16 192.168.10.0/24	MonitoingVMs	80 (HTTP)
Deny	DenyAllInbound	Any	Any	Any

Recap of security options

Securing Access From Internet

DDoS Protection for public IP addresses

Intelligent DDoS Protection

Application Gateway/Web Application Firewall

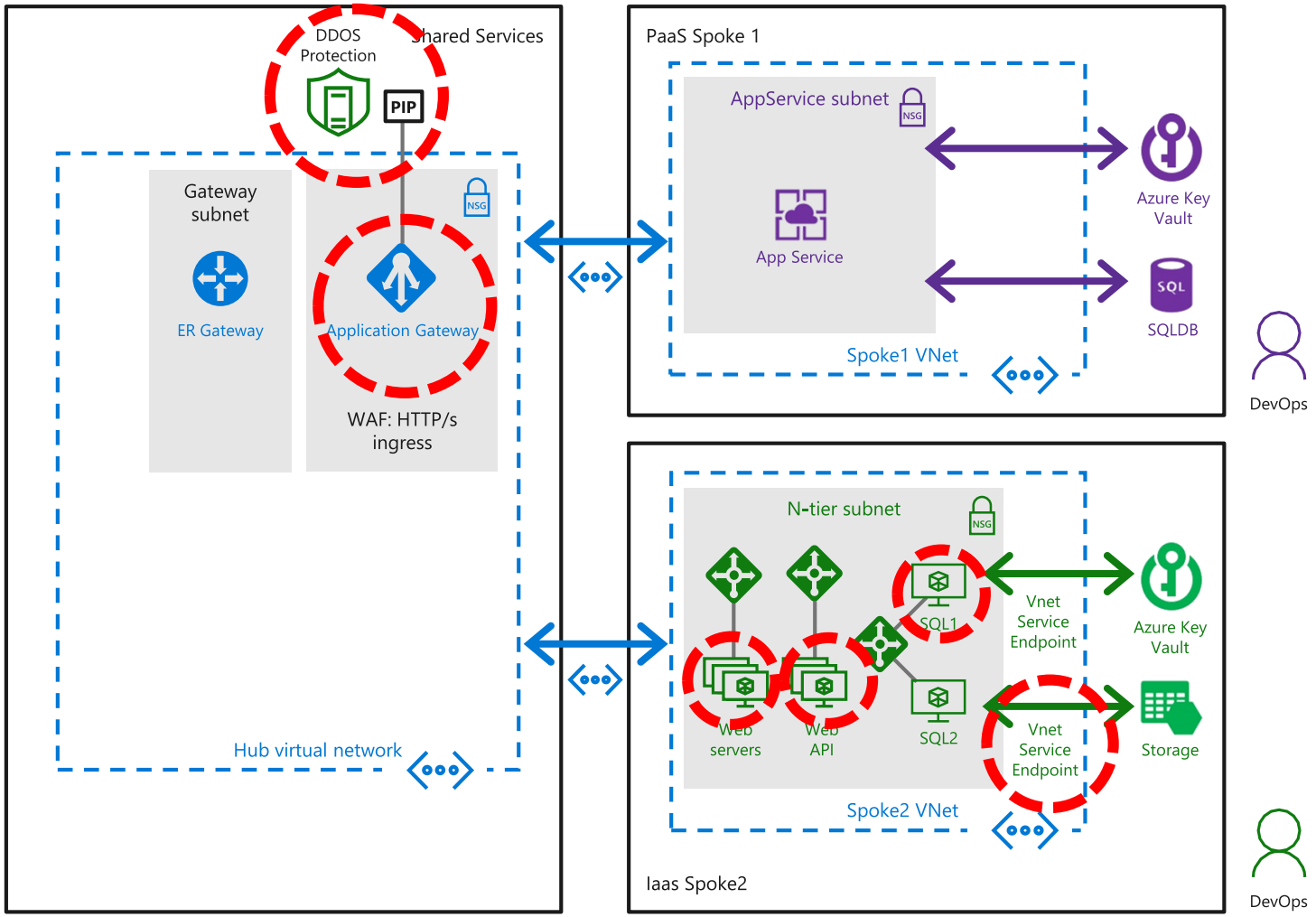
Web application protection

Network and Application Security Groups

VNet network security with micro-segmentation

Service Endpoints

Azure PaaS resource protection



Securing access from my Virtual Network

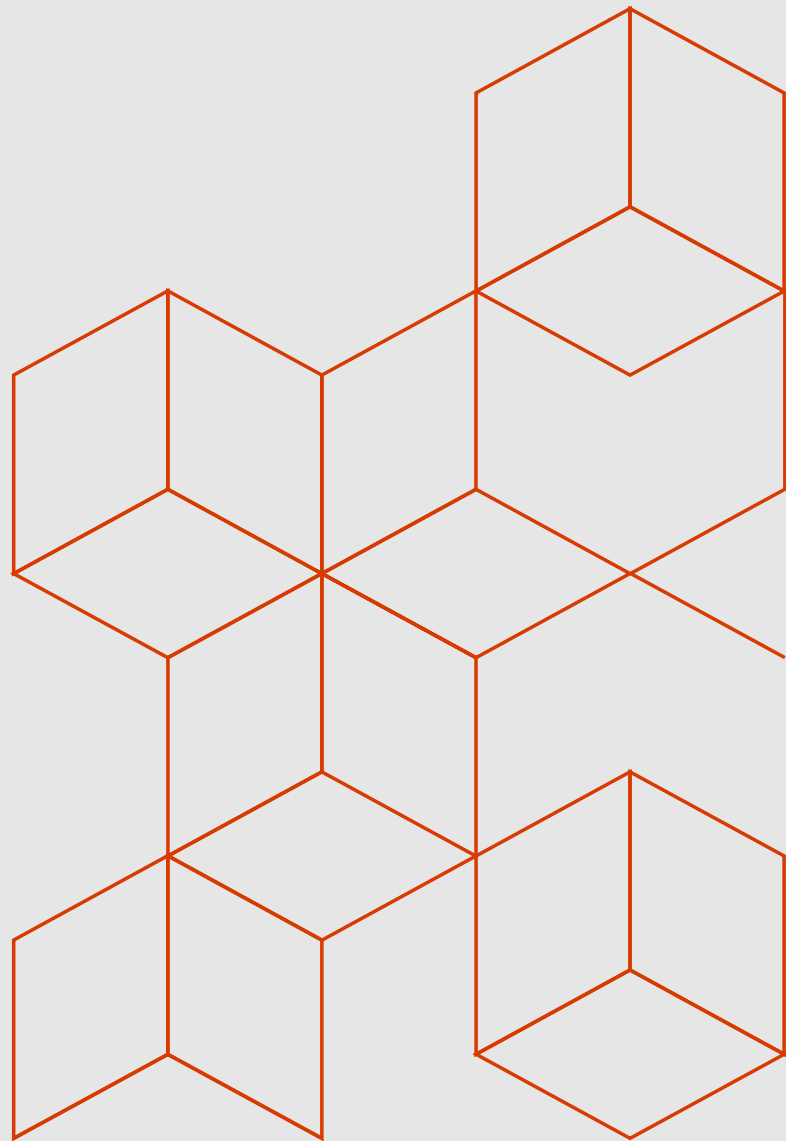
Potential threats

✔ **Unrestricted inbound traffic**

How to prevent access from DMZ to private zones, other applications or on premises network?

Unrestricted outbound traffic

How to prevent access to untrusted destinations, downloads of malware, stealing data on the internet…?



Advanced outbound filtering options

Routing

- Default routes for all VNet traffic
- User defined routes for L7 filtering

Network Virtual Appliances

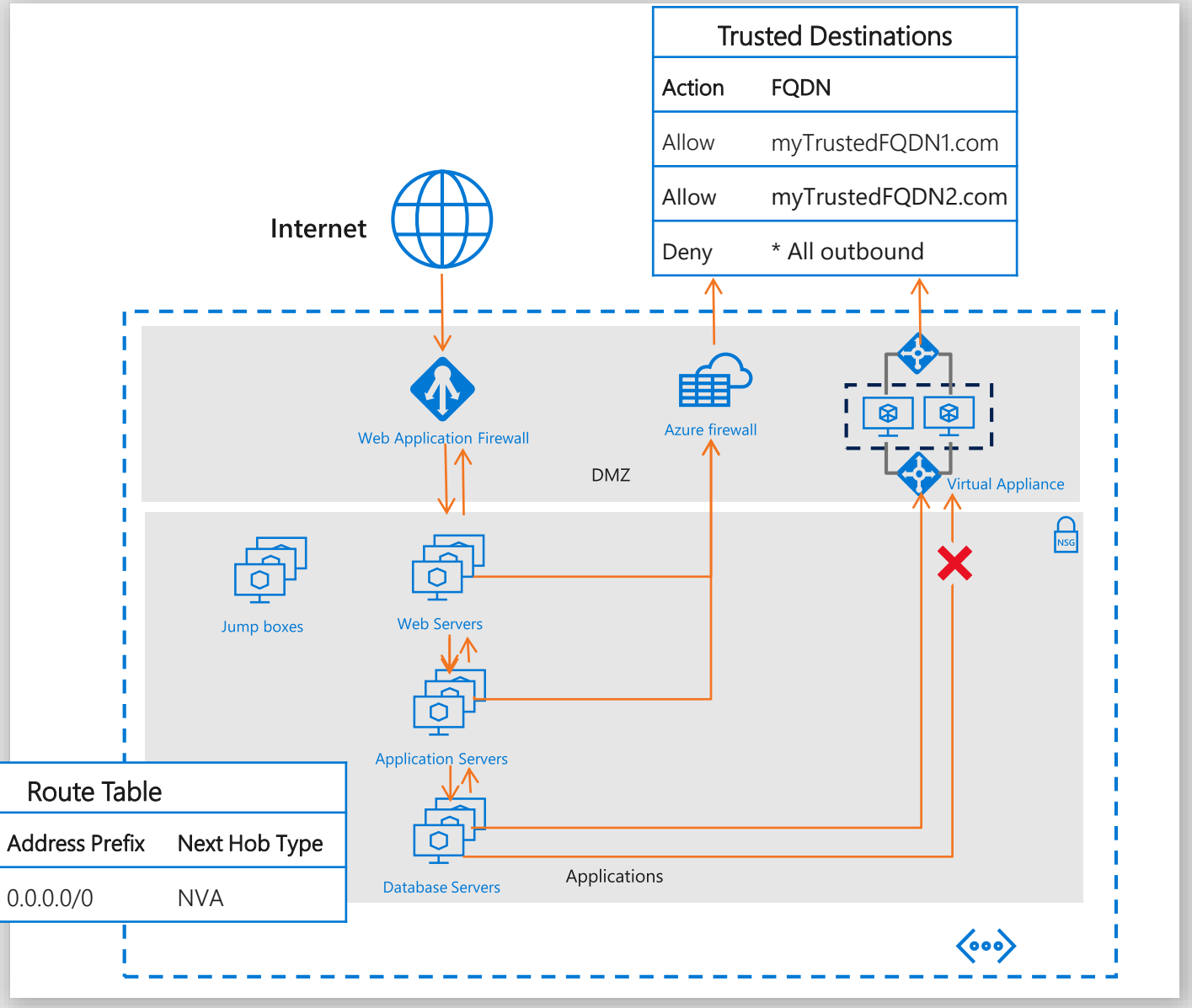
- Rich eco-system of partners with familiar products
- Deep integrations with on premises and other clouds

Azure Firewall

- FQDN filtering for internet traffic
- Integrated with Azure products

Service Endpoint Policies

- Optimal routing for data services
- Simplified policy definition



Azure Firewall

GA

Cloud native stateful Firewall as a service

Central governance of all traffic flows

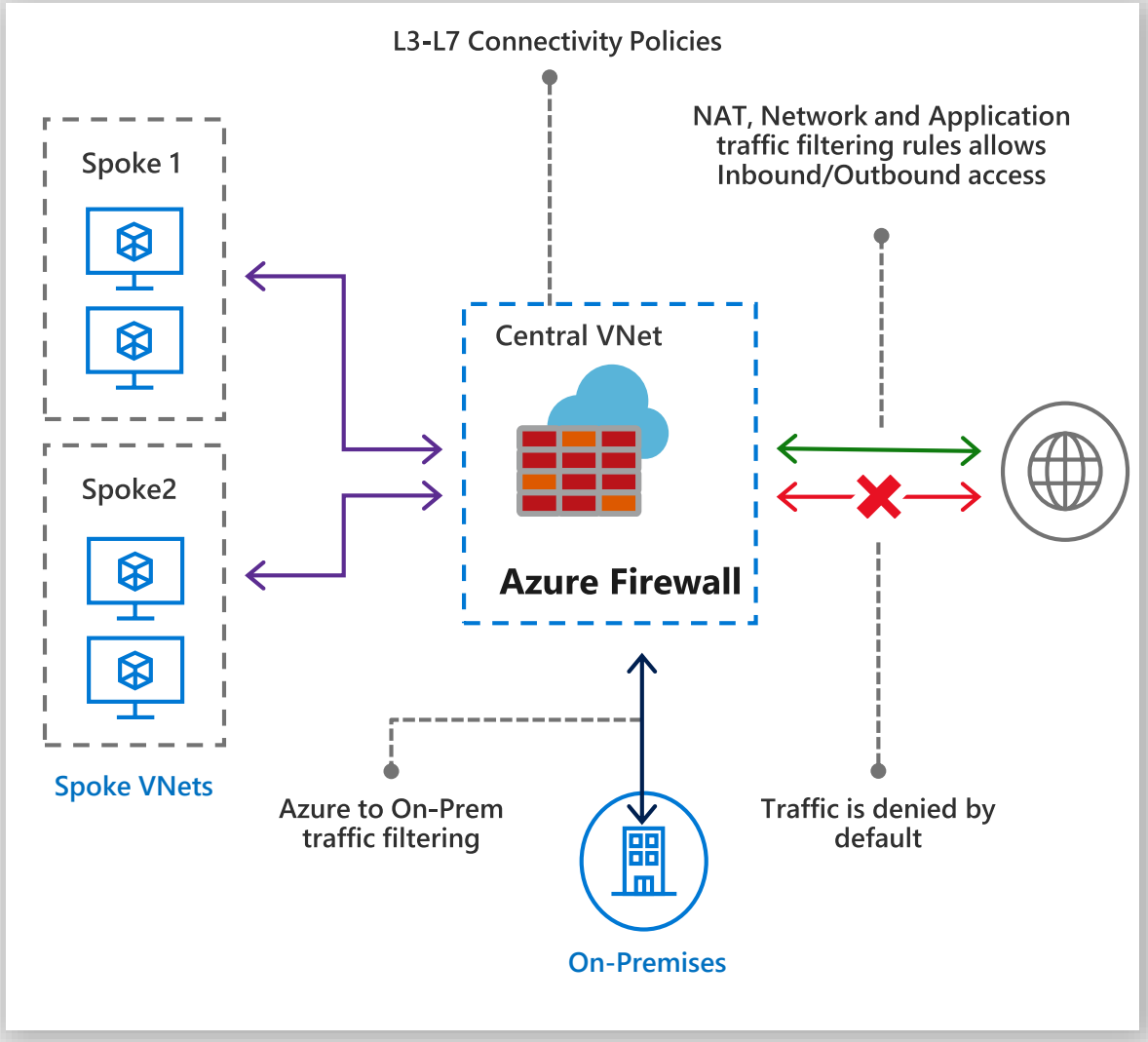
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice



Summary of security options

Securing Access

DDoS Protection for public IP addresses

Intelligent DDoS Protection

Application Gateway/Web Application Firewall

Web application protection

Network and Application Security Groups

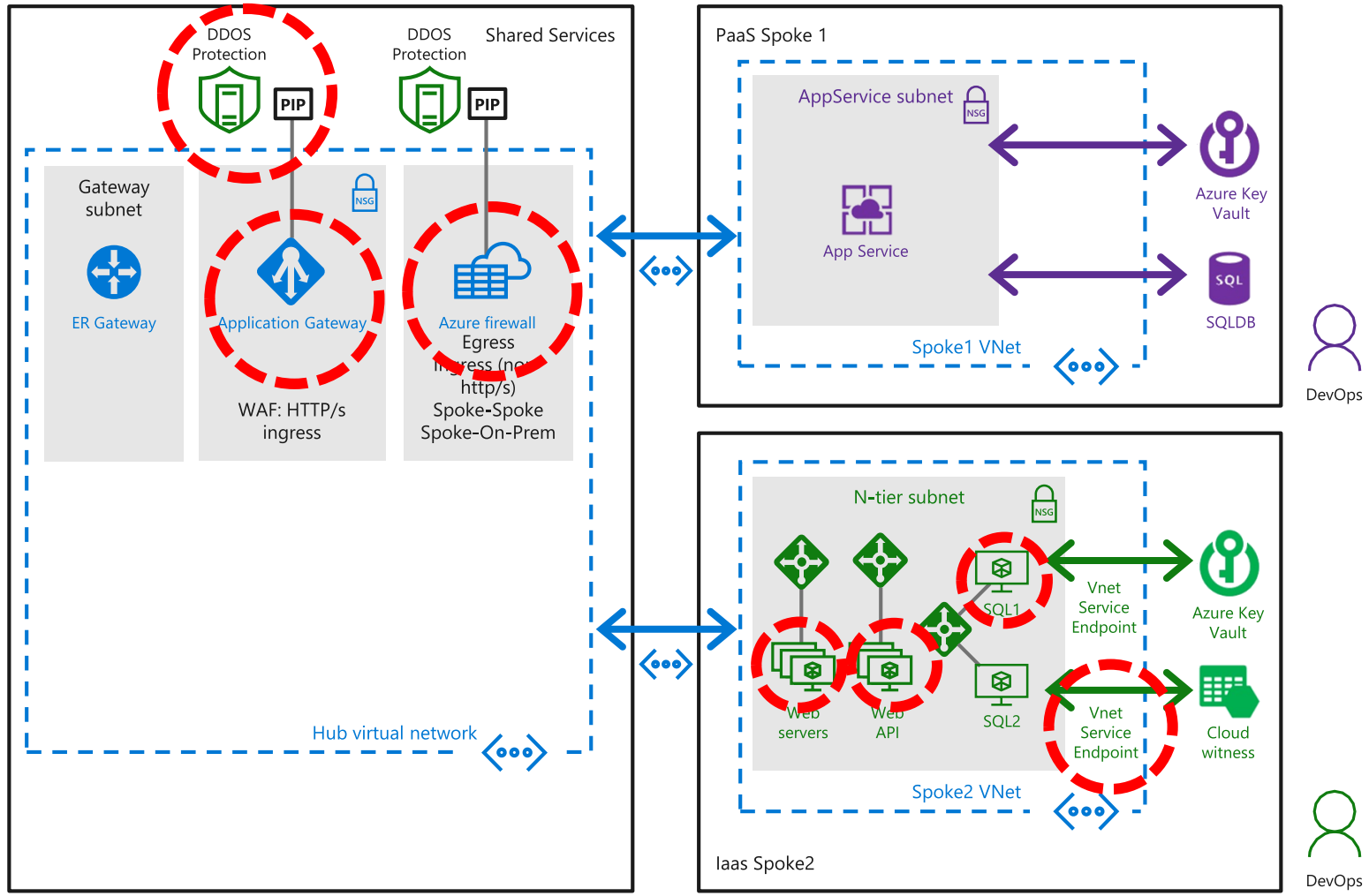
VNet network security with micro-segmentation

Azure Firewall

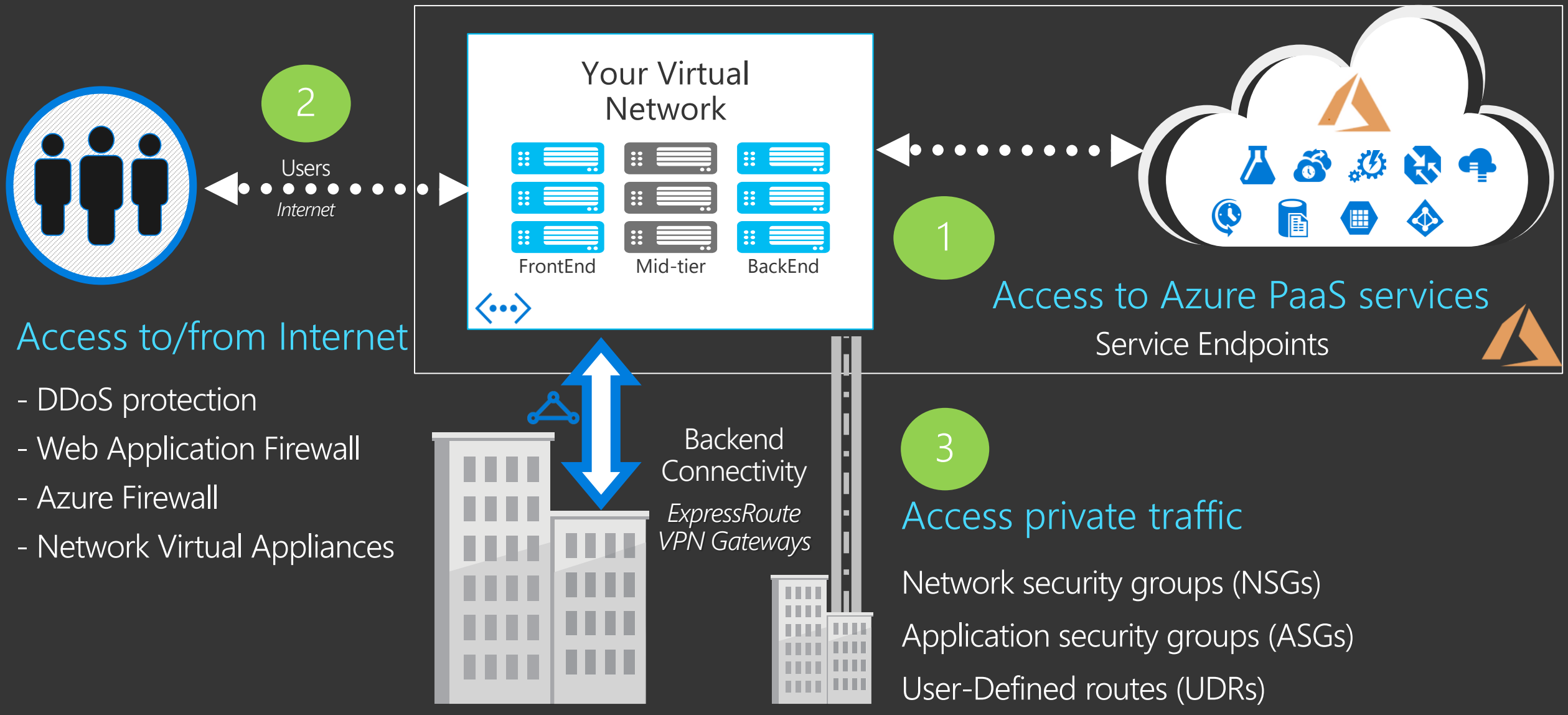
Full egress and ingress (non-http/s) controls

Service Endpoints

Azure PaaS resource protection



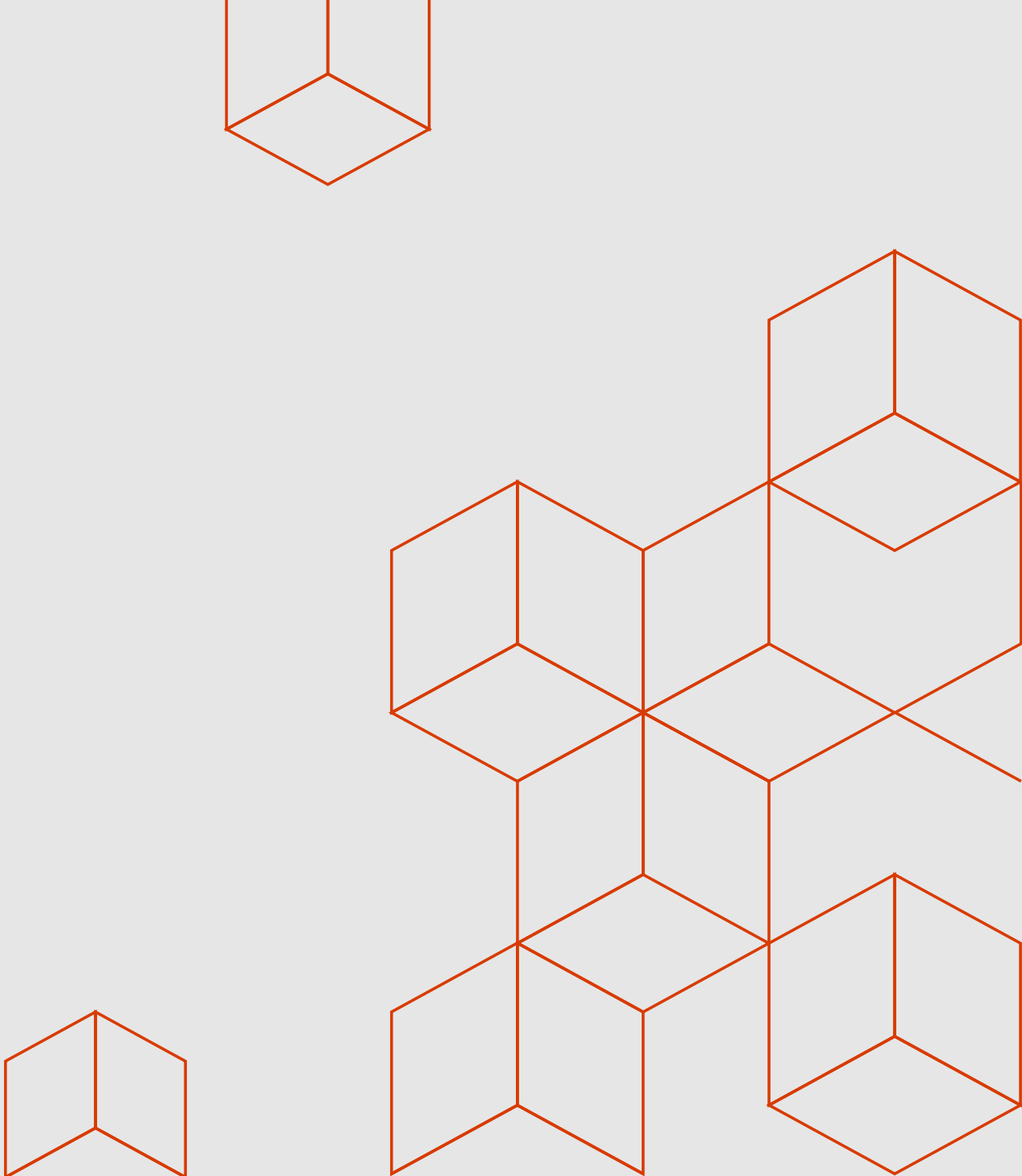
Application Access Patterns



Access to/from Internet

- DDoS protection
- Web Application Firewall
- Azure Firewall
- Network Virtual Appliances

Putting all together



Planning network security for your mission critical workloads

Potential threats

- ✓ **Access to Azure PaaS services from untrusted networks**
  - How to protect my PaaS resources from being access from anywhere?
- ✓ **Preventing data exfiltration from my Azure PaaS services**
  - How to protect my data from being copied to other accounts?
- ✓ **DDoS Attacks**
  - How to protect my internet exposed workloads from DDoS attacks?
- ✓ **Web Application vulnerabilities**
  - How to prevent exploit of common vulnerabilities on my web applications?
- ✓ **Unrestricted inbound traffic**
  - How to prevent access from DMZ to private zones, other applications or on premises network?
- ✓ **Unrestricted outbound traffic**
  - How to prevent access to untrusted destinations, downloads of malware, stealing data on the internet…?

Azure Network Security Portfolio

DDoS protection

High availability for your applications with protection from excess IP traffic charges

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Prevent SQL injection, stop cross site scripting and an array of other types of attacks using cloud native approach

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

Better central governance of all traffic flows, full devops integration using cloud native high availability with autoscale

Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering

Security Groups

Full granular distributed end node control at VM/subnet for all network traffic flows

Distributed inbound & outbound network (L3-L4) traffic filtering on VM, Container or subnet

Service Endpoints

Extend your Virtual Network controls to lock down Azure service resources (PaaS) access

Restrict access to Azure service resources (PaaS) to only your Virtual Network

Key Takeaways

- Pick network security offerings based on application access patterns
- Layer security by mix-and-match based on your requirements
- Scale the security model, as your workloads scale